GLOBAL COMMAND AND CONTROL SYSTEM (GCCS)

SYSTEM AND NETWORK MANAGEMENT

CONCEPT OF OPERATIONS (CONOPS)

Version 1.8.2

16 December 1996

GCCS Configuration Management
Document Number: LL-500-189-02

Distribution Unlimited

Document is UNCLASSIFIED in its entirety

Defense Information Systems Agency
Joint Interoperability and Engineering Organization
Defense Information Infrastructure (DII)
GCCS Engineering Office
Engineering Division (JEJ)
45335 Vintage Park Plaza
Sterling, Virginia 20166-6701

Intentionally Left Blank

SIGNATURE SHEET

The Global Command and Control System (GCCS), System and Network Management, Concept of Operations (CONOPS), Version 1.8.2 is:

SUBMITTED BY:

_____

John Gauss, RADM, USN
Deputy Director
Joint Interoperability and Engineering Organization
Defense Information Systems Agency

APPROVED BY:

_____

Douglas D. Buchholz, LTG, USA
Director for C4 Systems
Joint Staff

CONCURRENCE SHEET

The following concur with the Global Command and Control System (GCCS), System and Network Management, Concept of Operations (CONOPS), Version 1.8.2:

Robert F. Paling, Col, USAF Product Group Manager Air Force Global Command and Control System	Barry E. Wright, COL, USA Project Manager Strategic and Theater Command & Control Systems
J. E. Vesely, Col, USMC Program Manager Marine Corps Systems Command	L. E. Cook, Capt, USN Director, Command and Control Systems Division

Abstract

A system must be managed. It will not manage itself.

"The Best of DEMING", collected by Ron McCoy, 1994

The sons and daughters of America serve to protect and defend our great nation. They deserve, expect, indeed demand the very best from their leadership. If the arm of that leadership, the GCCS, falters, slips, or fails, we fail, and soldiers, sailors, airmen, and marines die. This is unacceptable.

Anonymous

Table of Contents

Questions or comments concerning the technical content of this document should be referred to the GCCS Chief Engineer, DISA/JIEO/JEXI, at (703) 735-8712 or DSN 653-8712.

List of Figures

List of Tables

GLOBAL COMMAND AND CONTROL SYSTEM (GCCS)
SYSTEM AND NETWORK MANAGEMENT
CONCEPT OF OPERATIONS (CONOPS)

1.0 INTRODUCTION

1.1 Document Structure

This document is divided into four major sections with each section being described briefly below. Also included, at the end of the document, are several appendices containing more detailed information relevant to the main body of the document. The four major sections of the document are:

Section 1, **INTRODUCTION**, which describes the objective and the outline of this document.

Section 2, **ANCILLARY ORGANIZATIONS ASSOCIATED WITH WWMCCS OR GCCS**, which describes the various organizations mentioned above and others that are crucial to understanding the GCCS environment. Specific areas addressed are the Defense Data Network (DDN) and its components, the Defense Information System Network (DISN) and its components of the Secret Internet Protocol Router Network (SIPRNET), the Integrated Tactical Strategic Data Networking (ITSDN) program, the communication servers, and the Worldwide Military Command and Control System (WWMCCS) management functions for the Joint Operations Planning and Execution System (JOPES), the WWMCCS Intercomputer Network (WIN) Network Operations Center (NOC), and other WWMCCS support offices. The goal of this section is to help the reader become familiar with these areas so one can better understand the changes that must occur.

Section 3, **GCCS ARCHITECTURE**, which describes the general GCCS Management Center (GMC) architecture. This section will describe the technical infrastructure being followed; the management functions to be performed; and the relationships of the GMC to the GCCS sites, the DISN, and the Defense Information Infrastructure (DII) management architectures.

Section 4, **GCCS OPERATIONAL MANAGEMENT RESPONSIBILITIES**, which describes the responsibilities and procedures to be used by the GCCS operational organizations.

A significant portion of the information presented in this document has been obtained from a number of other documents. These documents are listed in the Reference section. These referenced documents should be consulted for further background information. Footnotes and specific references have not been included.

If there is a discrepancy between this document or in the event of a conflict between the text of this

document and the references cited herein, contact the GCCS Chief Engineer in the DISA Center for Computer System Engineering (DISA/JEX) at DSN 653-8712 or commercial (703)-735-8712.

1.2 Background

The GCCS is our nation's conventional, joint command and control (C2) system. The GCCS is an organized assembly of C2 forces and elements organized to form the national C2 organization via a near instantaneously flexible system that collects, transports, processes, disseminates, and protects C2 information. It supports warfighting actions that are essential to the National Command Authorities (NCA) and subordinate elements in the generation and decisive application of national power. The GCCS operates over a global network employing communications, computers, force deployment planning and execution, surveillance, reconnaissance, intelligence, and space based systems to perform the C2 mission. Emphasis is placed on interoperability, C2 protection, counter C2 operations, and force deployment planning, and execution. Other information related systems and activities, their associated resources and technologies are also used to support the GCCS mission.

The GCCS is being implemented in accordance with the concept of operations of the Command, Control, Communications, Computers, and Intelligence (C4I) for the Warrior (C4IFTW) program. Validated by the Secretary of Defense and Chairman, Joint Chiefs of Staff (CJCS), C4IFTW establishes the objective of interoperability among forces, with a focus on the joint warfighter. The creation of a solid foundation embedded in strategy, policy, and doctrine has clearly created a new way of doing business in developing, acquiring, testing, and employing C4I systems. The GCCS takes advantage of these characteristics and provides warfighters with a global, flexible, and interoperable command and control system.

The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6721.01 dated 18 February 1995 defines the GCCS as:

> A comprehensive, worldwide network of systems which will provide the NCA, Joint Staff, combatant and functional unified commands, Services, Defense agencies, Joint Task Forces and their Service components, and others with information processing and dissemination capabilities necessary to conduct C2 of forces. GCCS is a means to implement the Command, Control, Communications, Computers, and Intelligence for the Warrior (C4IFTW) concept. An evolutionary implementation strategy is being used to provide warfighters with their required operational capabilities. The GCCS no grand design philosophy lends itself to extensive user participation, incremental fielding, and shorter periods between update cycles.

The GCCS provides platforms that will support forces for joint and combined operations throughout the spectrum of conflict anytime and anywhere in the world with compatible, interoperable, and integrated C4I systems. The GCCS incorporates the policies, procedures, reporting structures, trained personnel, automated information processing systems, and connectivity to provide information necessary to plan, deploy, sustain, and employ forces. It supports the range of operations along the

military continuum as envisioned by national military strategy. It also allows for responses to natural emergencies and/or man-made disasters when military support is appropriate and directed to respond.

1.3 Purpose

The purpose of the *Global Command and Control System (GCCS), System and Network Management, Concept of Operations (CONOPS)* is to identify the relationships among those Department of Defense (DoD) organizations with system and network management responsibility for the GCCS. Only by understanding the complexity and diversity of existing organizations and future system and network requirements for the GCCS can one appreciate the task at hand.

This document takes into account existing WWMCCS offices which perform specific types of management functions on WWMCCS today and how the roles of these offices must change to support the expanded requirements of the GCCS. This includes the Defense Information Systems Agency (DISA), Joint Staff Support Center (JSSC) (DISA/WESTHEM/JSSC) responsible for the JOPES, the WIN NOC also operated by DISA/WESTHEM/JSSC, and other DISA offices that will be discussed later in this document.

Also included in this document are programs and/or organizations which are outside of the GCCS spectrum of operations, but upon which GCCS relies heavily. For example, the GCCS uses the SIPRNET, which is part of the DISN for its wide area network (WAN) data transport. The Defense Information Infrastructure Control Centers (referred to as the Global Control Center (GCC) and the Regional Control Centers (RCCs)) have no direct responsibility for GCCS assets, but they do control the SIPRNET WAN. It is important to understand how the hierarchical responsibilities of the different management centers must interact in order to create the most effective communications environment across which America's command and control operations can be conducted. An important aspect of the DISN is the ITSDN capabilities deployed today. These capabilities provide strategic gateways to tactical forces, C2 or otherwise, to reach back to sustaining units, organizations, or bases. Another capability available on the SIPRNET are communication servers which provide network connectivity for the DoD dial-in community via Secure Telephone Unit III (STU-III) access. Again, this capability could be used by mobile GCCS users to gain network connectivity via telephone systems. Finally, the GCCS must be aware of how the GCCS and the DISN will interface into the DII concepts of the future. It is extremely important that activities involving network and system management for the GCCS community be interoperable with the goals and structure of the DII.

Unlike WWMCCS today, the GCCS is not an all inclusive operation. The GCCS of today's warfighters operates at two different system high classification levels instead of the single, top secret system high environment of the WWMCCS. Ninety-five percent of all data and applications on WWMCCS were downgraded to the secret or lower classification level to operate on the GCCS. Only five percent remained at the top secret level supported by a residual system of the WWMCCS operations referred to as the Top Secret Support System (TS3). This system high classification split

within the GCCS will complicate system and network management by requiring two separate system high levels within the management system. In the beginning, the system and network management functions for the top secret system high portion of the GCCS (TS3 and future GCCS(T)) will be minimal in the new GMC. The replacement of the mainframes with new hardware, coupled with a new system architecture is referred to as the GCCS(T) for the top secret portion of the GCCS. The TS3 will continue to be supported by existing WWMCCS management systems. However, after the top secret Honeywell mainframes supporting TS3 are replaced with modern Sun servers in GCCS(T), the system and network management requirements will increase at the GMC. Eventually, with further development and the proliferation of Multi-Level Security (MLS) devices and Compartmented Mode Workstations (CMW), the system high secret and top secret requirements of the GCCS user may be combined onto a single platform.

The GMC is composed of three major locations with supporting offices. The sites are the GMC-Pentagon, located in the Pentagon and operated by the DISA Joint Staff Support Center (DISA/WEY) personnel functioning in close proximity to the National Military Command Center (NMCC). JSSC can provide the NMCC with the immediate status as to the health of the GCCS. The GMC-Site R location is also operated by JSSC personnel and serves as the backup for the GMC-Pentagon. The GMC-Site R is off of the Alternate NMCC (ANMCC) located at Site R in northern Maryland. And finally, the GMC-OSF operating at the DISA Operational Support Facility (OSF) located in Sterling, Virginia run by DISA GCCS Engineering personnel. The GMC will provide 24 hours a day, 7 days a week, operational support for managing the GCCS.

A discussion of the roles and responsibilities of the WWMCCS and other DoD organizations listed above is included in section 2 of this document to provide a strong foundation on which this document is premised. Armed with this information, the document will then define the GCCS Management Center both in functional and operational terms. The GMC will evolve from existing WWMCCS support organizations, the initial OSF GCCS Hotline, and new assets. All existing organizations will undergo several stages of transition in order to meet the demands of the GCCS system and network management requirements. The primary goal is for the GMC to reach initial operating capability (IOC) when the GCCS achieves IOC after Operation Test Readiness Review Phase 2 (OTRR2). However, the GMC and GCCS IOC dates are not mutually inclusive. It is during the parallel testing period of GCCS and WWMCCS that the users will be evaluating the functionality of the GCCS before WWMCCS is shut off.

The DISA Joint Staff Support Center is responsible for writing the *Global Command and Control System (GCCS), System and Network Management, Implementation Plan* which will identify the technical and day-to-day operational requirements for execution of this CONOPS. Additionally, the DISA JSSC will be responsible for establishing the software, hardware, and manpower infrastructure necessary for carrying out the concepts and procedures in this CONOPS.

2.0 ANCILLARY ORGANIZATIONS ASSOCIATED WITH WWMCCS OR GCCS

2.1 Defense Data Network (DDN)

The DDN consists of four packet switched networks which are identified according to the highest classification level of the data transported. The networks are the Military Network (MILNET) at the unclassified but sensitive level, the Defense Secure Network One (DSNET1) at the secret level, the Defense Secure Network Two (DSNET2) at the top secret level, and the Defense Secure Network Three (DSNET3) at the top secret/sensitive compartmented information classification level. These networks were constructed utilizing the ARPANET packet switching technology. Initially, wide area service of up to 64 kilobits per second (kbps) was provided to two classes of subscribers. These classes were the asynchronous "dumb" terminals and then hosts via the ARPANET-Host Interface Protocol (AHIP). Subsequent host access service was augmented by a DDN-specific version of the CCITT X.25 protocol (DDN Standard) and by the CCITT basic X.25 protocol.

DSNET2 is the top secret DDN network that the WWMCCS community enjoys exclusive use of for data transport. The DDN is a 12-year initiative that expired on 15 October 1995. A contract extension was negotiated to extend the DSNET2 portion of the DDN to support the WWMCCS until the GCCS is the on-line C2 system. With the successful downgrade of the WWMCCS and the migration of functions to the GCCS, most of our national C2 operations have migrated to the secret level. The DSNET2 can be turned off at the same time as WWMCCS because data transport for the GCCS will be provided by the Secret Internet Protocol Router Network (SIPRNET) of the DISN. However, three nodes of WWMCCS Honeywell equipment will be kept operational to support the remaining top secret mission requirement of the GCCS referred to as TS3. DSNET2 will not be required by TS3 because that system also uses the SIPRNET for data transport through End-to-End Encryption (E^3) devices. Some network management functionality of DSNET2 were kept after the 15 October 1995 time frame to provide interim support to this residual system high top secret requirement of TS3. Once TS3 has migrated to GCCS(T) this functionality will be included in the GMC.

2.2 Defense Information System Network (DISN)

The DISN is a collection of voice and data networks composed of multiplexers, cryptographic devices, routers, and other devices combined to create a worldwide information transfer infrastructure. The DISN evolved from two directions. The first was the need to replace the DDN. The second was a study conducted in September, 1991 by the Office of the Assistant Secretary of Defense for C3I (OASD/C3I). The study directed DISA to implement the recommendations of an OASD/C3I chaired Task Force which had investigated alternatives for the evolving DoD communications. The five major goals were:

- Establish a foundation for providing subscriber-to-subscriber transport service infrastructure

- Consolidate independent DoD networks into a transport service for providing

interoperability, resource sharing and consolidation
- Provide faster provisioning and more responsive customer support
- Capitalize on commercial-off-the-shelf (COTS) products and international standards to create an open, non-proprietary architecture
- Reduce DoD telecommunications costs

One of the data portions of the DISN is comprised of router based layers, each of a different classification level. The three-layer router model of the DISN does not directly correlate to the four data layers of the DDN described earlier. The unclassified router layer is the Unclassified Internet Protocol Router Network (NIPRNET) which replaces the MILNET. The secret router layer is the Secret Internet Protocol Router Network (SIPRNET) discussed earlier which replaces DSNET1. No top secret router network will be built to replace DSNET2. With the downgrading of 95% of our nations C2 WWMCCS functionality to secret, no DoD organization currently requires a stand-alone, robust, physically separate, top secret Wide Area Network (WAN). However, several communities of interest will require a global top secret WAN-like capability. This will be provided by tunnelling through one of the other DISN networks (NIPRNET or SIPRNET). Those customers requiring top secret datagram transport will use end-to-end encryption (E^3) devices for encrypting the datagrams. These encrypted top secret datagrams can then use the SIPRNET for data transport. The final layer is the top secret/sensitive compartmented information router network called the Joint Worldwide Intelligence Communications System (JWICS) that is replacing DSNET3. This network currently is not under DISA control. It is owned by the Defense Intelligence Agency (DIA). The possible migration of JWICS from DIA to the DISA DISN is currently being staffed in DISA, no agreements have been reached by DISA and the DIA though future plans call for this network to become a component of the DISN.

Figure 1 shows the router layers of one segment of the data portion of the DISN's overall architecture. Each layer is shown as a separate entity. There exists certified multi-level security (MLS) cryptographic devices that will allow for data of one classification level to ride on a different DISN router layer for data transport. An example is the group of secret-level Air Force (AF) subscribers who use the unclassified router layer (NIPRNET) for their data transport. The AF community uses the BLACKER E^3 system and operates under this scenario. A BLACKER gateway has been placed between NIPRNET and SIPRNET to allow AF networks behind BLACKER devices to communicate with other secret level users on SIPRNET. However, the AF is no longer pursuing the use of BLACKER devices in their communications architectures though the capabilities are available. Another example is the TS3 portion of GCCS. The TS3 sites operate at the top secret layer but use SIPRNET for data transport. This is accomplished by using the Motorola Network Encryption System (NES) which is another E^3 system. The GCCS community must be aware of the existence of these E^3 capabilities. They play an important role in how C2 users are all interconnected in the virtual network. Their existence in the system and technical operating parameters must be understood so proper management of the GCCS can be performed.

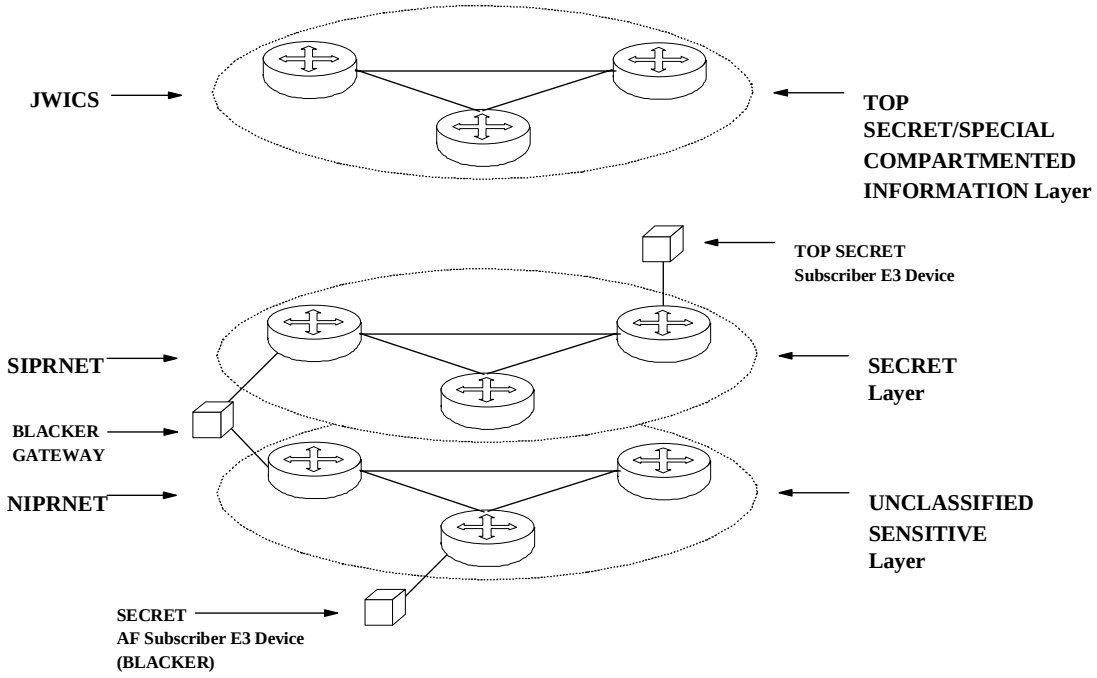


Figure 1 DISN Internet Protocol Router Layer Architecture

2.2.1 DISN Network Management Hierarchy Model

The DISN uses a three-layer model to define the different areas of network management responsibility. Figure 2 graphically depicts the model while concentrating on the SIPRNET viewpoint. The top level DII control center is referred to as the Global Control Center (GCC) which is operated by the DISA C4I Network Systems Management Division (D31). The GCC provides management oversight for the networks of the DII for which DISA has network management responsibility. These networks include the SIPRNET, the NIPRNET, the defense satellite networks, the Network Equipment Technologies, Inc. Integrated Digital Network Exchange (IDNX) multiplexer networks, the Defense Switch Network (voice), AUTODIN, and others to name a few. The second layer is comprised of the Regional Control Centers (RCCs). The RCCs are responsible for the day-to-day operations of the networks under their immediate control. They are geographically oriented with several centers dispersed across the United States; a center located at the DISA European facilities to cover Europe, and another located at the DISA Pacific facilities to cover the Pacific assets. The RCCs are responsible for the DISA assets within their areas and operate as peers to each other. The RCCs responsible for various portions of the NIPRNET and SIPRNET are also

responsible for the health of the DISN routers installed on those networks. The Scott AFB RCC is responsible for the IDNX multiplexer network.

The RCCs and the GCC are responsible for DISA assets only. They do not control any assets owned by the individual Service/Agencies (S/As) connected to the networks or WANs. The GCCS premise routers are included in the list of equipment that the GCC and the RCCs do not manage. It is the responsibility of the GCCS community, i.e., the individual sites or support organizations, to manage these assets. This is where the third layer of the hierarchy model comes in to play. These management centers, or DII control centers, are referred to as Local Control Centers (LCCs) and they belong to the individual subscriber communities. In the case of the GCCS, the community must establish LCCs to manage the GCCS assets. This LCC concept as it relates to the GCCS will be explained in greater detail later.

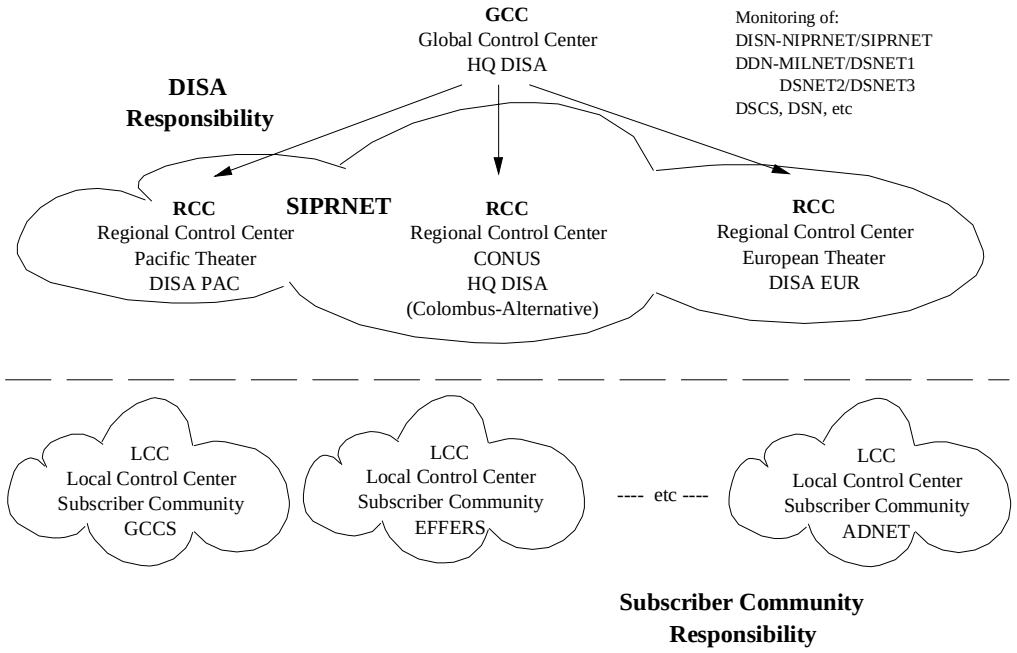


Figure 2 DISN Network Management Hierarchy Model

2.2.2 DISN Management Demarcation Point

The major concern of system and network management responsibilities is determining where the demarcation point exists between GCCS communications equipment and the DISN's SIPRNET. This has been discussed in terms of physical locations, management control, and the ownership of the communications equipment. As alluded to before, the DISA GCC and RCCs do not manage assets belonging to subscriber communities, in this case the GCCS. While this definition provides a starting

point, it does not provide the exact physical location of change over. The demarcation point for serial access circuits has been defined more completely by stating the RED (unencrypted, clear-text classified information) side of the cryptographic equipment in the subscriber's location is where DISA GCC and RCCs responsibilities end and the subscriber's responsibility begins. This is because the DISN RCCs are responsible for the health and maintenance of the serial access circuits. Typically, DISN cryptographic and other ancillary devices are located in the subscriber's area. Arrangements are made during the provisioning process on how the DISN owned equipment will be maintained. In the case of Ethernet connections, the subscriber's responsibility is from the servicing Ethernet port on the SIPRNET backbone router to their assets. The SIPRNET RCCs do not manage the GCCS site's Local Area Network (LAN). It is possible that a site with an Ethernet connection to the SIPRNET can still have a premise router in the communications path. To reenforce these definitions, Figures 3 and 4 are included to show the demarcation points. The two drawings help show how the demarcation point differs for the two types of connections. Again, the primary difference is the SIPRNET RCCs are responsible for restoration of the serial access circuits. Approximately 95% of the GCCS to the SIPRNET access connections are serial in nature with the other 5% being Ethernet.

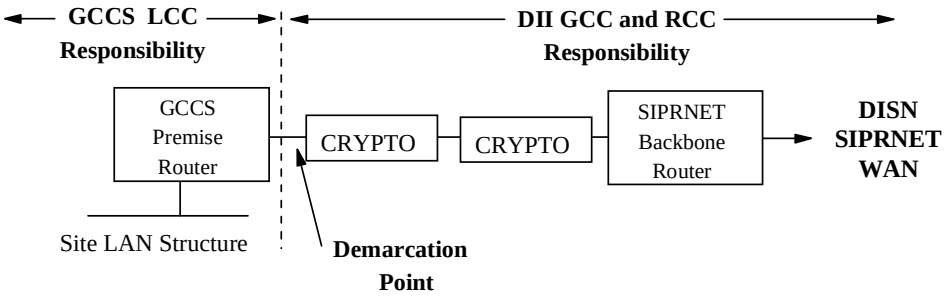


Figure 3 Demarcation Point of Responsibility for Serial Access Circuits to DISN Networks

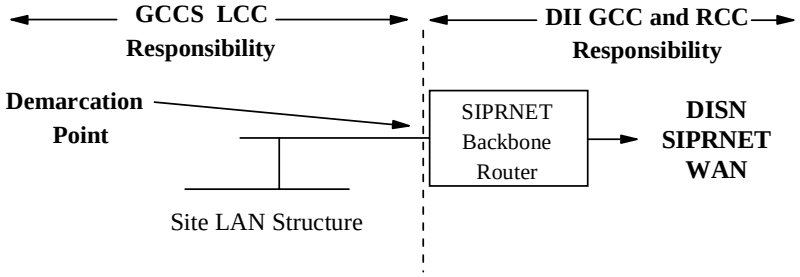


Figure 4
Demarcation Point of Responsibility for Ethernet Access to DISN Networks

Figure 5 provides a logical demarcation representation for the physical demarcation show in Figure 3. The top portion of the drawings shows the seven layers of the Open Systems Interconnection (OSI) reference model for protocol definitions. Across the bottom of the drawing is a physical connectivity drawing similar to that of Figure 3. However, Figure 5 really shows two copies of Figure 3 back-to-back to show how an actual GCCS site would be interlinked to another GCCS site. In the middle of the drawing is the breakdown of who manages which portions of the link. The SIPRNET RCCs are responsible for their WAN routers and the access circuits to those routers. The local sites are responsible for their premise routers and their local site LANs. The GCCS Management Center operating out of the Pentagon has monitoring oversight for all GCCS functionality across the globe. This can be interpreted by realizing the GMC has oversight from the application on one end system to the application on another end system.

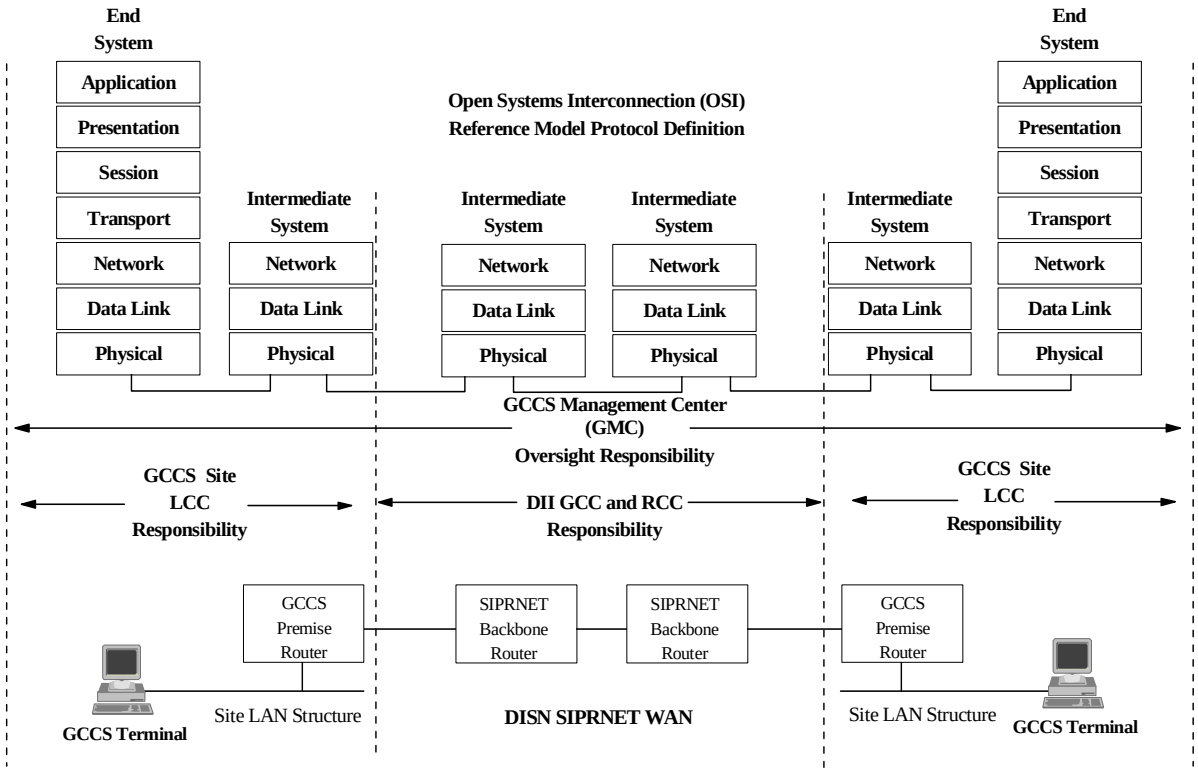


Figure 5 Logical Demarcation Points of Responsibility Based on OSI Protocol Model

The previous diagrams reflect a pure demarcation between the DISN SIPRNET WAN and the GCCS community. The DISN SIPRNET now offers management of customer premise equipment of a fee-for-service basis. The current fee is $50/month for premise routers. These rates are subject to change each fiscal year. The DISA/D343 office should be contacted for current information.

2.3 Secret Internet Protocol Router Network (SIPRNET)

The SIPRNET is the worldwide router-based network replacing the older X.25-based packet switched network DSNET1 of the DDN. The initial SIPRNET backbone router network went online 3 March 1994. Subscribers started coming online shortly thereafter. The SIPRNET WAN currently (as of 17 March 1996) consists of a collection of 45 operational backbone routers interconnected by high-speed serial links to serve the long-haul data transport needs of secret-level DoD subscribers. Eight additional SIPRNET backbone routers are in the planning and provisioning stage to meet increased customer requirements. SIPRNET supports the DoD standard Transmission Control Protocol/Internet Protocol (TCP/IP) protocol service. Provisions are made in the described SIPRNET architecture to support the Government Open Systems Interconnection Profile (GOSIP) router protocol service at a future date. Currently, no subscribers require immediate GOSIP protocol service on the SIPRNET. Subscribers within the DoD and other Government Agencies are able to use the SIPRNET for passing datagrams at the Secret-US Controlled classification level. The Secret-Not Releasable to Foreign Nationals (SECRET-NOFORN) classification level was removed from the SIPRNET in late CY95. Additionally, the NOFORN caveat has been changed to U.S. ONLY in security classification guidance documentation. There will be instances where connections to agencies of foreign governments or to other networks of a different classification level exist. These connections will be via an accredited security guard device that will prevent unauthorized or accidental disclosure of NOFORN or other caveated classified information from the SIPRNET.

The GCCS community relies heavily on the SIPRNET for its WAN infrastructure. As such it is imperative that a strong working relationship exists among the SIPRNET RCCs, the GCCS sites, and the GMC for the GCCS community. It is also important to note that unlike the WWMCCS environment and DSNET2, the GCCS does not enjoy exclusive use of the SIPRNET. The GCCS community only makes up about 15% of the subscribers on the SIPRNET.

The SIPRNET is managed by the DII/DISN RCCs which provide day-to-day operational management. The RCCs use Hewlett Packard (HP) Openview, CiscoWorks, and other management products to evaluate any router on the SIPRNET. Data is collected on various traffic patterns within the SIPRNET. Data collection includes total router traffic sent and received. The amount of Internet Protocol (IP) traffic from outside the WAN structure is referred to as the exterior load. Finally, system delays (elapsed times) are measured between all routers and ports using the PING tool. Measurements are in packets per second terms. The results of the various data collecting efforts are kept on file for long term management of the router-to-router traffic.

Appendix A contains additional information on the SIPRNET. It includes a complete site listing and topography maps showing the WAN interconnections at the time this document was published. For current information on the SIPRNET concerning programmatic or planning issues contact the DISA/D343 office at commercial (703)-735-8290 or DSN 653-8290. For operational issues please contact the DISA/D343 office at commercial (703)-735-8068 or DSN 653-8068.

2.4 SIPRNET Support Center (SSC)

The SIPRNET Support Center (SSC) operates at the system high secret level and went operational on the 28th of July, 1995. Foreign entities using the SIPRNET for data transport will not have access to the SSC. The SSC provides services that are similar to the unclassified DoD Network Information Center (NIC) that exists for the unclassified community. The SSC will meet the needs of the secret level DoD community by providing a multitude of Value Added Services (VAS). These services include domain name service registration, host name service registration, e-mail user registration, a WhoIs function, and other services. The SSC has several operational role accounts. They can be reached via e-mail at the following accounts:

Registrar	registrar@ssc.smil.mil
Hostmaster	hostmaster@ssc.smil.mil
Security	security@ssc.smil.mil
SSC	ssc@ssc.smil.mil
Service	service@ssc.smil.mil

The SSC WhoIs search capability is available on the World Wide Web page at *http://ssc.smil.mil/cgi-bin/whois*. The SSC can be contacted by telephone at 1-800-582-2567 or 1-703-802-8202. An unclassified FAX machine is available at (703) 802-8376. The SSC can also be reached via unclassified e-mail at siprnet@nic.ddn.mil. More information on the SSC can be obtained from the SIPRNET Project Officer at the DISA/D343 office via commercial telephone at (703)-735-8290 or DSN 653-8290.

2.5 Integrated Tactical Strategic Data Networking (ITSDN)

The ITSDN Quick Fix Program installed gateway routers to support deployed Joint Task Force (JTF) contingencies, exercises, and training missions with requirements to interface with the DISN Internet Protocol Routers (IPRs). The goal of the DoD, in general, and the ITSDN gateway routers, specifically, is to be able to support two contingency operations in different parts of the world simultaneously. The program installed 2 routers at each of 10 globally located strategic Ground Mobile Force (GMF) entry points. The 20 gateway routers are divided into 2 sets of 10 routers each based on the classification of data they process. The first set of routers will connect tactical subscribers to strategic networks via the SIPRNET. The other set of routers will connect tactical subscribers to strategic networks via the unclassified level wide-area backbone router system called the NIPRNET. Each entry point will receive two routers, one unclassified and the other secret. The

ITSDN routers support the standard TCP/IP protocol suite for serial or Ethernet connections. SIPRNET and NIPRNET are two of the IP router layers previously defined in the DISN router architecture model.

The ITSDN entry point suite of equipment consists of an unclassified router, a secret router, cryptographic equipment, and other ancillary devices. The 10 suites of equipment allow tactical forces access to strategic systems via the Defense Satellite Communications System (DSCS) through a Defense Communications System Entry Point (DCS-EP). These EPs provide worldwide access for JTFs. Some documents being produced may refer to the DCS-EPs as Defense Information System Network Entry Points (DISN-EPs). Both are valid. Additionally, the DCS-EPs are undergoing upgrades. Once an upgrade is complete, the location is referred to as a DISN Standardized Tactical Entry Point (STEP).

The tactical subscriber connections will be serial connections provided by satellite communications equipment at the DCS-EP sites. The ITSDN gateway routers support the standard TCP/IP protocol suite for serial connections to the gateway routers.

Deployed GCCS forces may rely on the ITSDN capabilities to reach the SIPRNET WAN. The DII/DISN RCCs provide day-to-day operational management of the ITSDN routers. Again, it is imperative that a strong working relationship exists between the RCCs and the GMC so the status of WAN assets supporting the deployed GCCS forces can be readily available.

Appendix B contains additional information on the ITSDN capabilities. Included is a site listing, a satellite coverage table, and other pertinent information. For current information on ITSDN concerning programmatic or planning issues contact the DISA/D343 office at commercial (703)-735-8355 or DSN 653-8355. For operational issues please contact the DISA/D343 office at commercial (703)-735-8068 or DSN 653-8068.

2.6 Dial-in Capabilities via SIPRNET Communications Servers (CSs)

Communications servers (CSs) were added to the SIPRNET during FY95 for the general DoD secret community though some sites are pending final activation. These CSs are managed by the DII/DISN RCCs responsible for managing the SIPRNET. The CSs give remote subscribers the capability to access the SIPRNET WAN via dial-in. This capability is especially valuable for those subscribers who do not have the need for a dedicated connection, for those subscribers who are continually traveling on temporary duty (TDY), or for deployed tactical subscribers who have access to a telephone system. The SIPRNET CSs are different than those being deployed by the GCCS program. The SIPRNET CSs are part of the DISN and fall under the control and management of the DII RCCs. The GCCS CSs are installed, controlled, and managed by the individual GCCS sites under the guidance of the GMC based on direction from the GCCS Engineering Department.

The SIPRNET CSs use AT&T STU-III Model 1910 to provide dedicated wireline encryption of the dial-in link. The CSs deployed on SIPRNET are Cisco 2511-CSs which are capable of 115 kbps

throughput on the dial in ports. However, the dial in link initially will be limited to a maximum throughput of 19.2 kbps to accommodate all makes and models of compatible secure telephone units (STUs) in use by the DoD. Higher throughput rates using compression algorithms will be made available on an incremental basis once the initial 19.2 kbps service has been fielded and fully activated. A maximum of 38.4 kbps compressed throughput can be realized by newer generation STUs using compression algorithms. The CSs are capable of supporting Point-to-Point Protocol (PPP), Compressed PPP (CPPP), Serial Line Interface Protocol (SLIP), Compressed SLIP (CSLIP), along with Telnet, Kermit, and other functions.

Both strategic and tactical GCCS forces can take advantage of the DISN CSs available on the SIPRNET WAN provided they are registered users. Again, the day-to-day operational management of the SIPRNET CSs will be by the DII/DISN RCCs. A strong working relationship between the RCCs and the GMC is required. Also, as security management is increasingly integrated with operations at the GCC and RCCs this working relationship must include the security managers. If GCCS users register for the SIPRNET dial-in service the DISN RCCs will be asked to provide the operational status of SIPRNET CS assets to the GMC through the peer-to-peer exchange of management data.

Appendix C contains additional information on the SIPRNET CSs. Included is a site listing and other information pertinent to the CS capabilities. It is important to note that like the DISN routers services, there is a fee for becoming a registered user of the DISN CSs. The published tariff is $10 per month per individual user with a one-time $45 registration fee. For current information on the SIPRNET CSs concerning programmatic or planning issues contact the DISA/D343 office at commercial (703)-735-8355 or DSN 653-8355. For operational issues please contact the DISA/D343 office at commercial (703)-735-8068 or DSN 653-8068.

2.7 Defense Information Infrastructure (DII) Control Concept (DIICC)

The goal of the DII program is to provide a seamless end-to-end integration of DoD's information resources. A unified view of all infrastructure components is to be provided by the DII Control Concept (DIICC). DIICC will provide a fused, real-time representation of the three-dimensional battle space. The wide range of DoD operations clearly demonstrate the need for a DIICC that is flexible enough to ensure and maintain mission integrity independent of geographical location or environment.

The DIICC takes a more open-systems view of information infrastructures. Figure 6 is a view of the systems and network management data flow between DII elements. Note that this view is non-hierarchical in nature. On the outer ring are the Base-level Network Control Centers (BNCCs), the Defense Satellite Communications System (DSCS), the System Management Centers (SMCs), the Local Control Centers (LCCs), etc. These various centers are the management information providers. The Management Information Bases (MIBs) and alerts from management software move inward to the RCCs and finally, after aggregation, to the GCC. Both the status information and aggregate information can be transmitted outward from the RCCs.

The DII/DISN GCC and RCCs depicted in Figure 6 are the responsibility of DISA DISN organization. Unfortunately, responsibility for the outer ring is not so clearly established. Some entities are under the responsibility of DISA while others are the responsibility of the subscriber communities or S/As. The GCCS program has the responsibility to establish its own LCC for system and network management of the GCCS assets. GCCS assets can be thought of as the hardware and software necessary to perform the C2 mission as defined by the Joint Staff GCCS program. A two-tiered concept is used for managing the GCCS with a Primary LCC taking care of the Joint Staff oversight mission with Secondary LCCs at the site locations performing the day-to-day operations. This two layer approach is explained in more detail later in the document. The major concern will be to ensure the direction taken by the GMC is in concert with the long term goals of the DIICC.

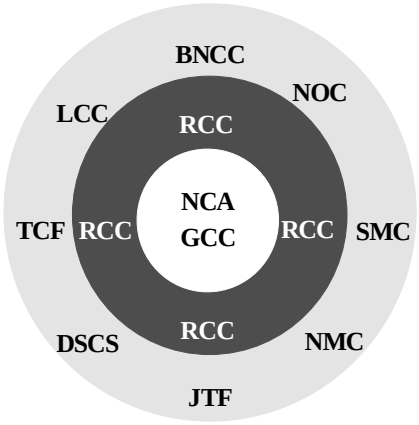


Figure 6 DIICC Management Information Data Flow

The DIICC system and network management strategy uses the OMNIPoint systems and network management model shown in Figure 7. The five management services defined by the International Standards Organization's (ISO) Common Management Information Protocol (CMIP) are shown in the middle of the figure. Feeding these services are service Delivery Points from commercial providers, Communications Elements (CEs), Information Processing Elements, Value-Added Services Elements, and the User Equipment Elements.

The essential DIICC value added is the correlation analysis function. The DIICC can make sense of seemingly unrelated inputs emanating from a wide variety of dispersed locations to isolate and determine the origin of a fault anywhere within the system. The DIICC can see all anomalies concurrently and proactively correlate the errors during the fault detection process. It can then broadcast to the appropriate parties the status of the problem and the steps being taken to fix it.

OMNIPoint was organized by the Network Management Forum (NMF). Its purpose is to analyze current standards and establish a progression of steps to specify the most robust systems and networks management possible. The focus for OMNIPoint is basic interoperability between systems and products for fault management and configuration management. The OMNIPoint partners have

selected standards and technologies that can be used in multiple combinations to support different environmental, budgetary, and functional requirements. Element managers, for example, use either the Simple Network Management Protocol (SNMP) or the Common Management Information Protocol (CMIP); both are specified. The OMNIPoint requirements reference technology from many different sources, such as Open Software Foundation (OSF), Distributed Computing Environment (DCE), the Object Management Group (OMG), Common Object Request Broker Architecture (CORBA), and the X/Open Management Protocol (XMP) communications interface. OMNIPoint defines several phases with each phase making progress towards a totally integrated and interoperable management structure.

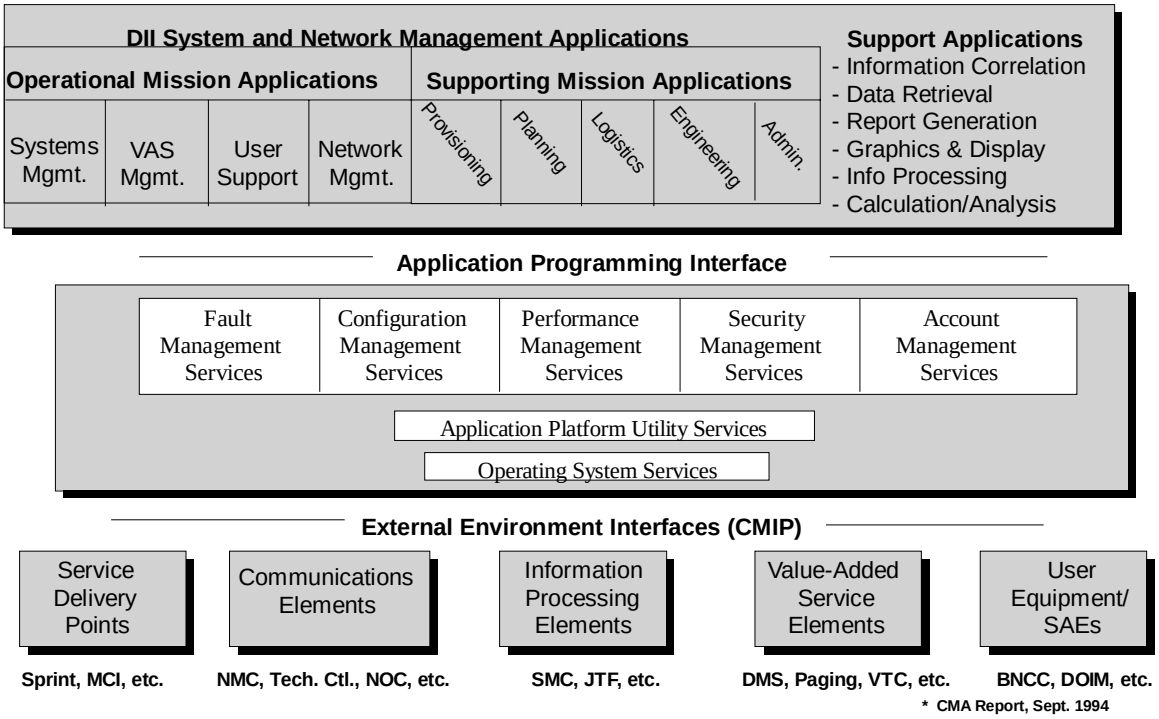


Figure 7 DIICC OMNIPoint Perspective*

The GMC being built for the GCCS community must be aware of future interactions with the DIICC. Additionally, the emphasis by DISA engineering and standards organizations to use the OMNIPoint approach across DoD also must be factored into the capabilities of the GMC. Only by properly looking to the future can the GCCS ensure it does not stovepipe itself into a system and network management corner.

Current information on the DII, the DIICC, and the OMNIPoint status can be obtained by contacting the DISA/D3 office at commercial (703)-735-6680 or DSN 653-6680.

2.8 DISA Joint Staff Support Center (JSSC) WWMCCS Management

Within the WWMCCS environment today are several main organizations and many site personnel charged with performing system or network management to keep the WWMCCS functioning. The main organization is DISA/WESTHEM/JSSC overseeing the Joint Operations Planning and Execution System (JOPES) and the WWMCCS Intercomputer Network (WIN) Network Operations Center (NOC). These offices exist at the Pentagon and are described below as they exist today in the WWMCCS environment. Later in the document the changing missions of these offices will be defined for the GCCS environment. Also included in the following sections are the JOPES Functional Database Managers (FDBMs) and the JOPES Technical Database Managers (TDBMs). These are some of the personnel responsible for keeping the WWMCCS operational.

2.8.1 Joint Operations Planning and Execution System (JOPES)

The JOPES is an operations planning and execution command and control system that provides timely deployment information shared throughout the Joint Planning and Execution Community (JPEC). The JOPES is a part of the WWMCCS and interfaces with the other automated data processing (ADP) systems both within and outside of the WWMCCS. The ADP component of JOPES is designed as a real-time, transaction-oriented, distributed database system. User entries generate transactions which update data in the local databases. Transactions are simultaneously transmitted to other sites over the WIN to update all sites which maintain the affected data. All JOPES system users must understand and carefully control the dynamic nature of this process to preclude unexpected or undesired results. To ensure that JOPES provides the JPEC with the critical information it requires, users must recognize that JOPES is a data repository and the utility and accuracy of its outputs are only as good as the quality and timeliness of input data from the deployment community. The viability of the JOPES database depends upon three major factors. They are:

- Maintenance of Time-Phased Force and Deployment Data (TPFDD) developed and refined during deliberate planning
- Timely and accurate information update by online user entry or automated interfaces during time-sensitive deployment planning and execution
- Control and management of the JOPES network update procedures to maintain data integrity and synchronization

2.8.1.1 Mission Support Services Division

The Mission Support Services Division is staffed by DISA/WESTHEM/JSSC personnel. This division is tasked with multiple functions in support of the JCS. One task the division is charged with is overall system management of the JOPES applications, JOPES Version 3.3.3, as they exist in WWMCCS today. Operations include local and network JOPES management, incident reporting, and backup procedures based on direction from the Joint Staff J-33 office at the Pentagon. System management of the JOPES applications within the GCCS will continue as a valid requirement. However, this system management requirement must be combined with the additional system management requirements of all GCCS applications. The changing nature of the Joint Staff

Operations Support Division will be explained later in the document. The following sections will explain some of the more important functions performed by this division.

2.8.1.2 GCCS Applications Branch (JOPES)

The GCCS Applications Branch (JOPES) is staffed by DISA/WESTHEM/JSSC. The branch monitors the JOPES network and provides technical support to ensure the continual operations of the JOPES network. This support includes the technical aspects of the transaction flow of the JOPES network and the performance of network and application software. This does not include support in functional matters or diagnosis and repair of problems in the JOPES software code. Specific responsibilities in WWMCCS were:

- Provide technical assistance on a continuous basis to include 24 hour operations as required
- Operate and maintain the JOPES application network and databases
- Analyze and correct operational anomalies
- Maintain a Ready Reference Library
- Prepare and install JOPES software release to include pre-release installation/testing; magnetic tape preparation and shipping; and planning and coordination with Joint Staff, network Functional managers and sites.
- Provide technical expertise to DISA, Joint Staff and other agencies as required
- Assist in Network testing
- Conduct network analyses of problems and monitor fixes that are installed
- Maintain JOPES transaction metrics
- Host TDBM Technical Interchange meetings and participate in other JOPES meetings as appropriate
- Chair the JOPESTECH teleconference

2.8.1.3 JOPES Functional Database Manager (FDBM)

In the WWMCCS environment, all JOPES Functional Database Managers (FDBMs) must be familiar with the critical, unique features of the JOPES database. The FDBM must understand the physical and practical limitations in loading Operational Plans (OPLANs) into the JOPES since the JOPES database is finite on a WWMCCS host. Prior to loading a TPFDD, the FDBM must determine the data will fit. Overfilling a database will result in an inoperative JOPES.

The WWMCCS JOPES database is divided into two distinct databases. One is for exercise data and the other is for real-world data. Each of these databases is further subdivided into eight subfiles. FDBMs are responsible for maintaining the integrity of these databases and their subfiles. The subfiles in the WWMCCS are:

Subfile Nomenclature	Series
Access Control/Sync	0-99
Plan Information (PI)	200
Unit Information (UI)	400
Requirements (REQ)	500
Scheduling and Movement (S&M)	600
Nonstandard Cargo (NSC)	700
Movement Table	800
Force Module (FM)	900

Table 1 WWMCCS JOPES Database Subfiles

Primary responsibility for JOPES functional management is shared between the network FDBM and the local site FDBM. Proper JOPES functional management requires every organization or installation using JOPES (as a fully configured JOPES site, through remote terminal access, or through automated interface) to designate a qualified FDBM. The DISA Direct Support Branch (WEY34) functions as the network FDBM.

The network FDBM responsibilities are broader in nature than those of the site FDBMs. In essence, the network FDBM is responsible for global system management of the JOPES. These responsibilities include but are not limited to the following activities listed below. These activities are for the JOPES existing in the WWMCCS environment. Changes will occur for the JOPES functionality in the GCCS environment. Specific network FDBM responsibilities in WWMCCS were:

- Initiate and synchronize network OPLANs
- Coordinate distribution of OPLAN data to JOPES network sites
- Change OPLAN type, distribution, or access. This function applies particularly to the management of limited access OPLANs to include their conversion to NORMAL status
- Manage functional analysis of JOPES software/hardware problems and develop fixes or workarounds
- Control timing and flow of network transactions
- Establish coordination requirements and procedures for site FMs
- Chair FM permanent teleconference (TLCF) for coordination with all site FMs
- Maintain synchronization among all JOPES databases
- Ensure JOPES supports the vital operational mission of strategic military deployment planning and execution under crisis conditions
- Develop joint directives necessary to establish standardized procedures, specific JOPES information and interface requirements to ensure flexible and responsive JOPES operation to support force and material movements

- Develop specific procedures to ensure continued operations during periods of degraded capability at the network hub sites. This includes ensuring the integrity and synchronization

of alternate databases, developing technical procedures for rerouting transactions to an alternate network hub site, and ensuring uninterrupted performance for the functional procedures of all JOPES management functions.

The JOPES resides on the Honeywell mainframe computers which are interconnected by the WIN Communications System (WINCS) using DSNET2. The JOPES software provides real-time transaction processing via the Interface Processor (IP) and the Update Processor (UP) modules. It is important to understand the manner in which JOPES databases are "networked" together using the WINCS. The following paragraphs will help describe the transaction flow at each JOPES site and across the WINCS.

The IP software provides the communications link for transmitting JOPES update transactions, including network transaction routing controls, between the various JOPES database sites. The UP places the transactions, along with routing header information, on the WIN send queue. The IP then reads the transactions from the send queue and writes them to the transaction database (TDB) file. The next transaction is selected from the TDB and transmitted over the WIN. The remote IP receives the transaction and places it on the WIN receiver queue if routed to the remote site and on its TDB for forwarding to other sites to which it is logically connected. A network status file update passes to all connected sites to acknowledge the transaction transmission across the network.

Changes were made to the WWMCCS JOPES network transaction flow so it no longer operates on a "central hub" theory. The central hub configuration had many stalled transactions and queues would build up due to a malfunctioning JOPES site in the flow process. Currently, transactions flow so that any site has multiple sites feeding it at a time. This allows a site to continue operations when other sites experience problems, preventing network stoppages due to "hub" site failures. Transactions pass through network and TDB files, updating and clearing as they pass, virtually eliminating the possibility of losing transactions. This type of network flow also allows the system to recover sites without undue delays. Figure 8 illustrates the JOPES network transaction flow as it exists in the WWMCCS environment. This topology will change for the GCCS environment.

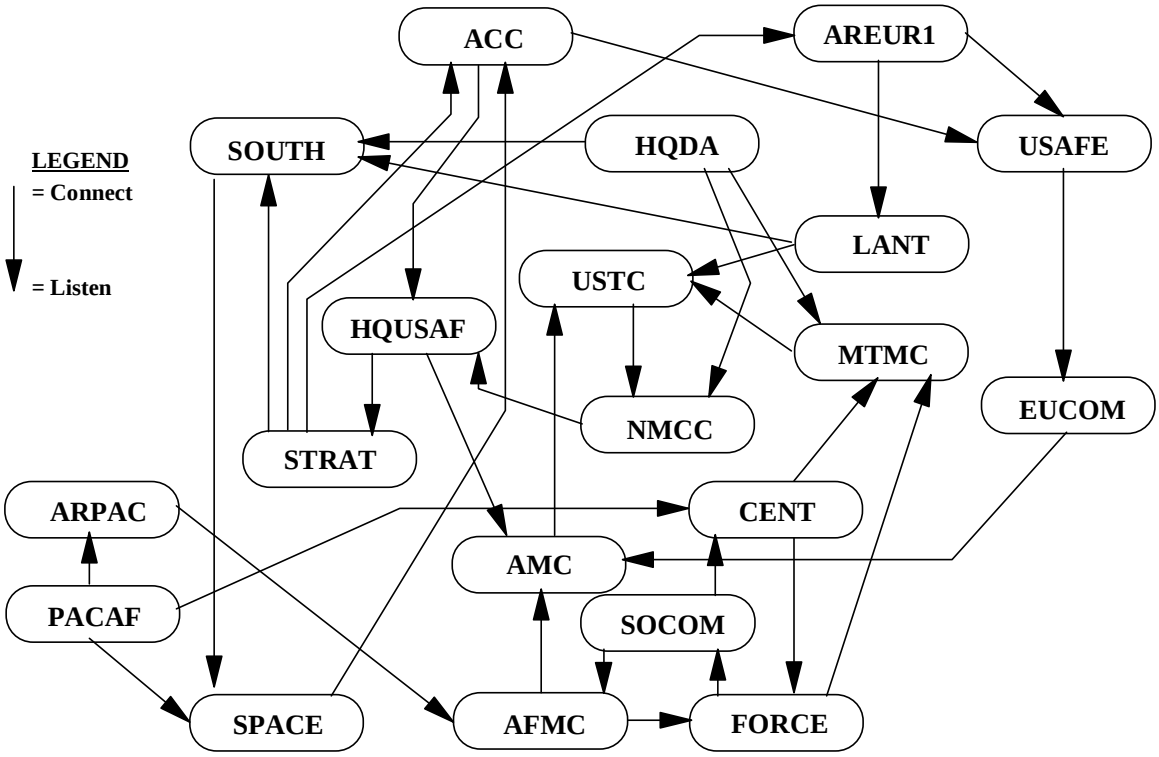


Figure 8 JOPES Network Transaction Flow Through the WINCS

Further information concerning existing JSSC operations can be obtained by contacting them at the GMC-HelpDesk.

2.8.1.4 JOPES Technical Database Manager (TDBM)

Primary responsibility for JOPES technical management is with the site Technical Database Managers (TDBMs) at the various WWMCCS host sites with direction from the Network Technical Database Management Section at the Pentagon. Corrective actions and procedures for the most common situations a TDBM may encounter are provided in the *Joint Operation Planning and Execution System (JOPES), Technical Database Manager's (TDBM), Handbook*, TD 18-64, 28 June 1993. The document also describes the tools that are available for the TDBMs to monitor and manage the JOPES in WWMCCS.

Again, for proper JOPES technical management under WWMCCS it requires every organization or installation using JOPES to designate a qualified TDBM. Internal coordination between the site TDBM and the FM is essential for ensuring the proper operation and health of the JOPES applications and database. The FM and TDBM cooperation is also essential to ensure proper access by users to the needed JOPES functions.

One of the duties of the site TDBM and FM is to be familiar with these procedures and be able to assist the WWMCCS ADP System Security Officer (WASSO) in registering new users for access. The subsequent granting and control of JOPES permissions is an FDBM and TDBM responsibility. Listed below are more TDBM responsibilities that exist in WWMCCS.

- Determine which five Person_IDs have permissions to add/delete users to JOPES
- Grants permissions to WWMCCS Standard Reference Files
- Grants Close Hold Plan Authorization and Registration
- Determine if system I/O gates are open or closed and functioning properly
- Initialize the JOPES Information Resource Manager allowing the site FM the JOPES "GRANT" permission required to use functions of the JOPES master menu
- Responds to and corrects database malfunctions detected via aborts of JOPES processes
- Responsible for resetting a plan status from "in use" back to "available"
- Monitor the automatic on-line backup process of the JOPES database
- Off-load held TDB transactions to disk during extended outage periods due to natural disasters, communications disruptions or extended computer failures.
- Perform saves of the JOPES database weekly
- Reload and recover a corrupted database
- Operate JOPES software utility programs to determine if any broken database chains exist in the JOPES database. Perform corrective actions to relink any broken chains.
- Perform disk pack analysis of files to determine which files must be rebuilt or restored

By working in close cooperation, the JSSC, the network FDBM, site FDBMs, the JOPES support personnel (TDBMs) at the Pentagon, and site TDBMs ensure that JOPES is available for the warfighting CINCs.

2.8.2 GCCS Applications Branch (SORTS)

The DISA Center for Computer System Engineering (DISA/JEX) is the technical OPR responsible for the Status of Resources and Training System (SORTS) application. The functional OPR is the Joint Staff, J-38, Readiness Division. The graphical user interface (GUI) application to access the SORTS data in the GCCS environment is called Global SORTS (GSORTS). The specific office responsible for day-to-day management of GSORTS is the JSSC GCCS Applications Branch (SORTS), Force Applications Section.

The Force Assessment Section provides many activities in support of the SORTS application. These activities range from day-to-day operations to developing and maintaining the application code. The following lists some of the responsibilities of the DISA/JEXAA office.

- Monitor/maintain the SORTS teleconference

- Monitor SORTS reporting
- Perform quality assurance checks on SORTS data
- Provide customer support
- Status reporting
- Provide backup/saves of Joint Staff database and reference files
- Register DoD, Joint Staff, and S/A units
- Maintain SORTS tables
- Maintain UIC communications file
- Provide database support to the USMC
- Update Joint Staff and GCCS databases

Like the JOPES supporting offices, the Force Assessment Section was performing system management for the SORTS application across the WWMCCS. Under the GMC umbrella, several of the responsibilities listed above will be moved to the GMC-Pentagon for operational responsibility. As such, the GMC-Pentagon will take over day-to-day operations requirements for the GCCS SORTS while the developers can continue to maintain the application and underlying support structure. The specific details for the day-to-day operations to be absorbed by the GMC-Pentagon are being determined.

2.9 Service/Agency and CINC Wide Area Network Management Organizations

The WWMCCS was supported by a single network, DSNET2 (operating X.25), interconnecting all of the mainframe sites. With the addition of the Host Access Units (HAUs) limited TCP/IP connections could be made to the mainframes. The communications architecture in the GCCS is significantly different. The GCCS uses TCP/IP technology which has greatly expanded capabilities over X.25. Everywhere in today's military and civilian worlds one finds TCP/IP in use. Military services and organizations have large supporting TCP/IP WAN networks. DoD consolidation efforts should see the eventual reduction of individual S/A and CINC WANs as they are absorbed into the DISN structure operated by DISA. However this will take time. These individual S/A and CINC WANs effect the GCCS because the system no longer has a single network interlinking all the sites together. The GCCS is supported by four major networks. The primary network is the DISN SIPRNET described earlier and all major S/A and CINC sites are connected to this network. However, the Air Force Command and Control Network (AFC2N) and the US Special Operations Command's SCAMPI network support a large number of smaller GCCS sites which are not directly connected to the SIPRNET. The use of multiple large WAN networks will greatly complicate the network management aspects of the GCCS. The increase in network complexity will make troubleshooting much more difficult. The key for successful management of the GCCS will rely on two major factors. The first is for all individuals to grasp the technologies and complexity of how the GCCS is interconnected. The other is for all managers at all levels to develop strong working relationships with their counterparts. WWMCCS has been in operation for almost two decades. Those involved are very familiar with the technologies and have the good working relationships in place. With time, the GCCS will reach the same stable position as the system matures and people become more knowledgeable. Further information is provided in the appendices on the AFC2N and

the SCAMPI networks.

3.0 GCCS ARCHITECTURE

3.1 Basis in Requirements

In *Joint Publication 1, Joint Warfare of the U.S. Armed Forces*, General Colin Powell, former Chairman of the Joint Chiefs of Staff, said that the ultimate goal of joint U.S. Forces interoperability is to ensure "every service can talk to every other service and every unit on the battlefield can talk to every other unit on the battlefield." Joint Publication 1-02 defines command and control as "the exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission." U.S. forces must be supported by a C2 system capable of augmenting the deployed force capabilities for wide-area surveillance, intelligence, battle management, and sustainment.

The GCCS is following the concept of C4I for the warrior (C4IFTW). The C4IFTW initiative mandates interoperability among forces, with a focus on the joint warfighter. The goal of the C4IFTW is improved command and control of joint warfighting. The C4IFTW Objective Concept started with the warrior's requirements and provided a road map to reach the objective of highly capable seamless, secure, interoperable global C4I support for the warrior. Joint mission effectiveness and reduced cost are key attributes of the concept. As part of the C4IFTW Objective Concept, the GCCS must be standardized, flexible, robust at any scale, and must present a common look and feel while adapting to the unique needs of each warrior.

The C4IFTW Objective Concept supports the planning, conduct, and support of joint, combined, and unified military operations that extend from the NCA to field tactical combat, combat support, and combat service support units. The concept presents a set of C4I infrastructure needs applicable across all levels of command. These needs include:

- A global C4I infrastructure must provide requisite modes of communications and automated C4I systems to satisfy warrior joint/combined information exchange and interface requirements at all levels of command
- A global C4I infrastructure must possess a reconfiguration capability
- The global C4I infrastructure must be capable of continuous operations in a communications constrained environment
- Current information must be provided in a timely manner from the global C4I infrastructure to the warrior on demand
- Information fusion and storage must be available at all warfighter levels
- A family of joint warfighter command and control terminal equipment must be available
- An end-to-end security capability must be provided within the global infrastructure
- The maximum degree of automation must be embedded in the process of the C4I infrastructure

- A global C4I infrastructure must conform to the Open System Interconnection (OSI) reference model and be based on national and international communications and database standards
- An optimized set of common procedures and databases must be developed
- Interoperability must be ensured via testing and configuration management

3.2 GCCS Infrastructure

Repeating the earlier definition, GCCS is a C4I system that supports forces for joint and combined operations throughout the spectrum of conflict anytime and anywhere in the world with compatible, interoperable, and integrated C4I Systems. This document emphasizes the "communications and computer" components and functions supporting C2. The GCCS "communications" are provided by the SIPRNET WAN, by S/A WANs such as the Air Force Command and Control Network (AFC2N), and by CINC and S/As LANs. Additionally, many secondary communications paths are provided by the individual S/As in support of their remote GCCS users. Both the WANs/LANs and the secondary communications paths take advantage of relatively stable telecommunications industry standards. The GCCS "computers" are provided by cooperative research and development efforts among DISA, the S/As, and other DoD organizations. Again, these platforms take advantage of evolving standards in the information systems industry. Together, the communications and computers of the GCCS will make up a part of the DII. The following sections will clarify both the software and hardware approaches taken by the GCCS to support the C2 mission. Emphasis will be placed on the communications and computer aspect.

3.2.1 Software Architecture

3.2.1.1 Generic Perspective

The GCCS is a distributed computing system. The software and data supporting command and control functions are distributed across heterogeneous and interoperable computers connected through the secret worldwide SIPRNET WAN. This distributed computing is implemented through a three-tier client-server architecture: the presentation (user-interface), the server (functional), and the data storage tiers. The presentation tier includes mission-specific joint, service, and command unique applications in addition to standard and commercial-off-the-shelf user interface elements such as X-Windows and Motif. The server tier includes functions (server-resident applications for mission applications, office automation, systems management, etc.), and the components upon which these functions reside. The data storage tier, linked to existing systems and applications, includes data storage and database management systems.

The goal of this approach is to insulate the application logic from the presentation and data storage software. The three-tier architecture, shown in Figure 9, addresses the issues of integrating object, relational, and legacy systems migrating to client-server technology. The three tiers, although pictured as three separate components, represent a logical separation and may reside on one, two, or more different hardware platforms.

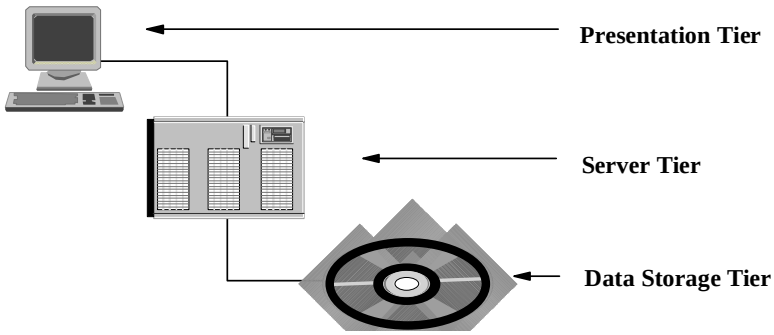


Figure 9 GCCS Three-tier Client-Server Structure

3.2.1.2 Defense Information Infrastructure (DII) Common Operating Environment (COE)

The following paragraphs were taken from the *Defense Information Infrastructure (DII), Common Operating Environment (COE), Integration and Runtime Specification (I&RTS), Version 2.0, dated October 23, 1995*. They will better explain the DII COE.

The DII COE originated with a simple observation about command and control systems: certain functions (mapping, track management, communication interfaces, etc.) are so fundamental that they are required for virtually every command and control system. Yet these functions are built over and over again in incompatible ways even when the requirements are the same, or vary only slightly, between systems. If these common functions could be extracted, implemented as a set of extensible low level building blocks, and made readily available to system designers, development schedules could be accelerated and substantial savings could be achieved through software reuse. Moreover, interoperability would be significantly improved because common software is used across systems for common functions.

This observation led to the development of the DII COE which is presently used in two systems: the Global Command and Control System (GCCS), and the Global Combat Support System (GCSS). Both systems use the same infrastructure and integration approach, and the same COE components for functions that are common.

Initial COE development was driven by the near-term requirement to build a suitable WWMCCS replacement. WWMCCS maintenance costs are significant and the system is rapidly reaching the point of technical obsolescence. A significant component of the COE challenge is to strategically position the system architecture so as to be able to take advantage of technological advances. At the same time, the system must not sacrifice quality, stability, or functionality already in the hands of the warrior. In keeping with current DoD trends, the COE emphasizes use of commercial products and standards where applicable to leverage investments made by commercial industry.

The cornerstone architectural concept jointly developed during the series of meetings in 1993 is the DII COE. The present COE is composed of software contributed from several candidate systems evaluated by this joint engineering team. It is being expanded to include global data management and workflow management for GCSS logistics applications. It will expand further as more functional areas desire to employ its services in areas such as Electronic Commerce/Electronic Data Interchange (EC/EDI), transportation, base support, personnel, health affairs, and finance.

An initial proof-of-concept system, GCCS 1.0, was created and installed in early 1994. GCCS 2.0 fielding began in early 1995 at a number of operational sites. GCCS 2.1 was fielded in mid-1995. The 2.0 series marks the real beginning of the DII COE concept. Its use is crucial in being able to rapidly integrate software from candidate programs to successfully build a baseline with an ever increasing level of functionality.

The DII COE has its roots in command and control, but the principles and implementation described in this document are not unique to GCCS nor GCSS. The principles and implementation are not limited to command and control or logistics applications, but are readily applicable to many other application areas. The specific software components selected for inclusion in the COE determine the mission areas that the COE can address.

The concepts represent the culmination of open systems evolutionary development from both industry and government with contributions from each of the services. The resulting COE architecture is an innovative framework for designing and building military systems. Because it reuses software contributed by service/agency programs, it utilizes field proven software for common C4I functions. The engineering procedures for adding new capabilities and integrating systems are mature, and have been used for several Navy JMCIS releases as well as in all GCCS production releases. The end result is a strategy for fielding systems with increased interoperability, reduced development time, increased operational capability, minimized technical obsolescence, minimized training requirements, and minimized life cycle costs.

The DII COE concept is a fundamentally new approach that is much broader in scope than simple software reuse. Software reuse itself is not a new idea. Unfortunately, most software reuse approaches to date have been less than satisfactory. Reuse approaches have generally emphasized the development of a large software repository from which designers may pick and choose modules, or elect to rebuild modules from scratch. It is not sufficient to have a large repository, and too much freedom of choice leads to interoperability problems and duplication of effort. This rapidly negates the advantages of software reuse.

The DII COE does emphasize both software reuse and interoperability, but its principles are more far reaching and innovative. The COE concept encompasses:

- an architecture and approach for building interoperable systems
- an infrastructure for supporting mission area applications
- a rigorous definition of the runtime execution environment

- a rigorous set of requirements for achieving COE compliance
- an automated toolset for enforcing COE principles and measuring COE compliance
- an automated process for software integration
- a collection of reusable software components
- an approach and methodology for software reuse
- a set of APIs for accessing COE components
- an electronic process for submitting/retrieving software components to/from the COE software repository

The COE must be understood as a multi-faceted concept. Proper understanding of how the many facets interact is important in appreciating the scope and power of the DII COE, and to avoid confusion in understanding COE material. The COE has three specific facets: the COE as a system foundation, the COE as an architecture, and the COE as an implementation strategy.

To view the COE as a C4I system is incorrect because it misses the fundamental point that the COE is *not* a system; it is a *foundation* for building an open system. This viewpoint also makes fielding and update schedules confusing because it fails to account for the impact of the evolutionary development strategy. To view the COE as GCCS or just an architecture gives the mistaken impression that its principles are limited to the GCCS program. GCCS is simply the first system build on top of the DII COE while GCSS is in progress. This view also fails to account for the fact that a baseline already exists composed of components selected from mature service/agency programs. Finally, to view the COE as just an implementation strategy is a limited perspective because it fails to account for the fact that there is a near term real world objective (WWMCCS replacement). It ignores the evolutionary nature of the COE and mission applications development, and it ignores the implied requirement to provide an easy update mechanism for operational sites.

Building a target system, such as GCCS or GCSS, is largely a matter of combining COE components with mission specific software. The COE infrastructure manages the flow of data through the system, both internally and externally. Mission specific software is mostly concerned with requesting data from the COE and then presenting it in a form that is most meaningful to the operator (e.g., as a pie chart, in tabular form, as a graph). The COE provides the necessary primitives for such data manipulation, and has the necessary information about where the requested data is stored, whether locally or remotely across the LAN/WAN. This frees the system designer to concentrate on meaningful data presentation and not on the mechanics of data manipulation, network communications, database storage, etc.

It must be kept in mind, however, that there is only one COE. Each system uses the same set of APIs to access common COE components, the same approach to integration, and the same set of tools for enforcing COE principles. Systems are built on top of the COE and use precisely the same COE software components, not just the same algorithms, for common functions (e.g., communications interfaces, dataflow management). This approach to software reuse significantly reduces interoperability problems because if the same software is used, it is not possible to have two systems that interpret or implement standards differently.

3.2.2 Hardware Architecture

Each of the GCCS sites has a core set of hardware for the GCCS software. Not all sites will have all components identified below. While some of the hardware directly correlates to the three-tiered client-server structure identified previously, other components are used to provide the GCCS communications infrastructure within each site. In addition, as the GCCS grows and matures the types and quantities of hardware (vendors, makes, and models) and hardware components (RAM, hard disks, PCMCIA slots, etc) will grow. The GCCS Engineering Office at DISA will make every effort possible to forecast future changes in hardware requirements to allow proper planning by GCCS sites. The following figure is representative of a typical GCCS site. The paragraphs after this diagram will be used to explain the functions of each hardware component within the GCCS suite of equipment.

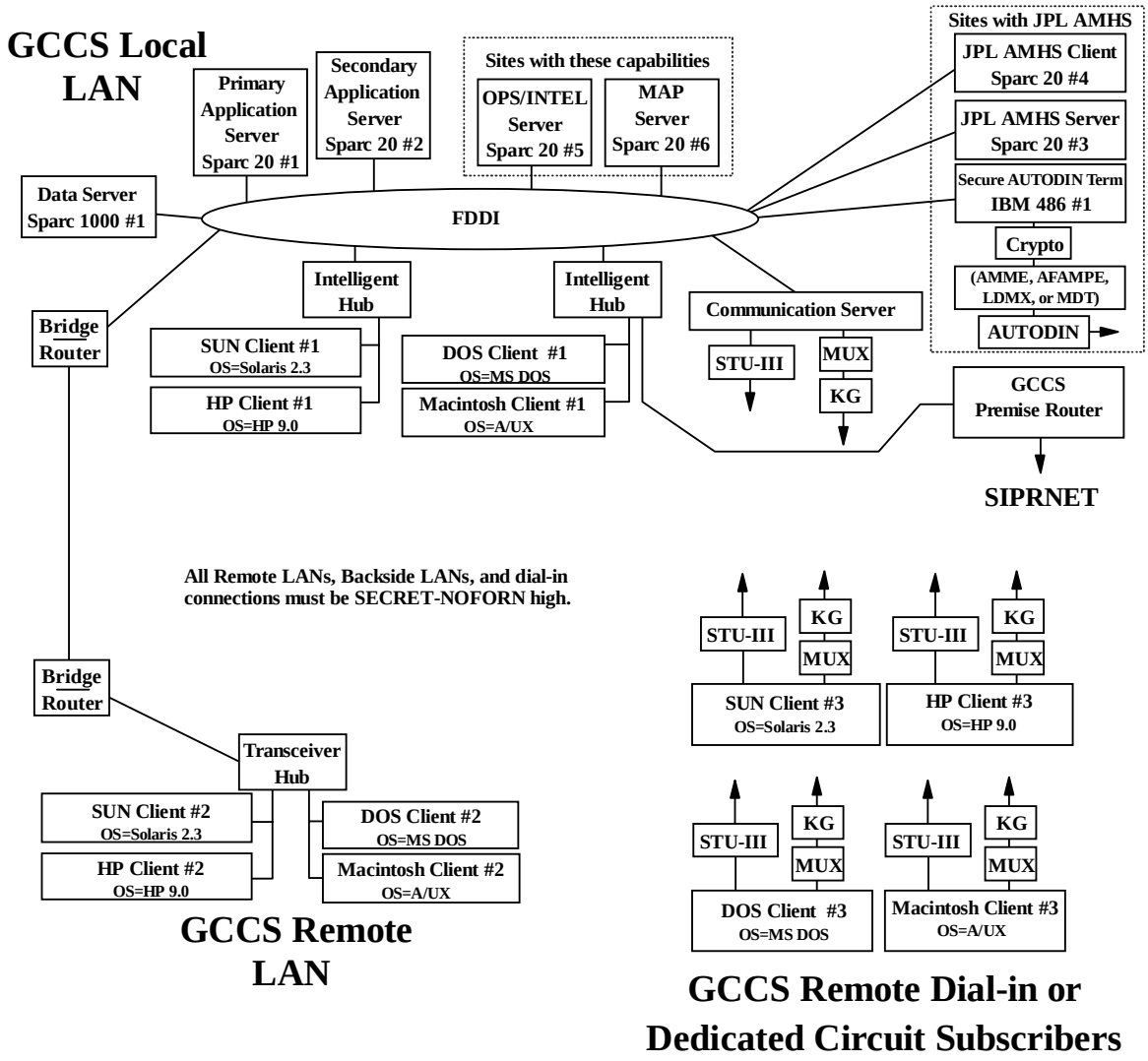


Figure 10 GCCS Site Hardware General Configuration

The data server represents the third tier, the data storage tier, in the software model. The typical data server is a Sun Sparc 1000 with at least 32 Gigabytes (GB) of mirrored storage from a RAID Array and 512 MBs of random access memory (RAM). Some of the GCCS sites have Sun Sparc 2000 instead of the Sparc 1000 for their data storage device. Variances in disk capacity and RAM size exist within the GCCS as a whole. Also, some sites have additional data servers installed to accommodate site or service unique data requirements.

The next set of devices are the application servers. These are initially Sun Sparc 20s with most servers having 4 GBs of hard disk storage and 224 MBs of RAM. They are the second tier, the server tier, in the software model. Initially, each IOC site was given two application servers. Depending on the size and complexity of the site, some sites now have up to 10 application servers. The original application servers were sized to support 5 concurrent XWindows sessions or 20 Telnet sessions. Individual differences in applications server's RAM and processor power will cause these numbers to fluctuate. Additionally, the specific size requirements for TAC-4s to act as application servers are still being determined.

The next device is an OPS/INTEL server. A few of the GCCS sites have been identified to receive an additional Sun Sparc 20 after GCCS IOC to serve in this capacity. The device has 4 GBs of hard disk storage and 224 MBs of RAM. Actual implementation of this capability is still being determined.

Next is the MAP server. Some GCCS sites have the need to store a large volume of maps at their location. A Sun Sparc 20 is identified to be this server and will be fielded after IOC. The hard disk size and amount of RAM required in this device is still being determined. One of the solutions being considered is for the 37 Joint Staff designated IOC sites to receive a basic CD-ROM library from the Defense Mapping Agency (DMA).

The next suite of equipment is the Automated Message Handling System (AMHS). The system being used is the one produced by the Jet Propulsion Laboratory (JPL) for the Army. The system is uniquely identified as the JPL AMHS, GCCS Configuration. In actuality, three configurations exist for the AMHS suite of equipment based on the hardware utilized for AMHS functionality. The first configuration consists of two Sun Sparc 20s. One serves as the primary AMHS server while the other is the AMHS dedicated client. The dedicated Sparc 20 client workstation represents the one used by the operator responsible for the AMHS. It should be noted that any of the GCCS workstations can be loaded with the AMHS client software. The second configuration consist of a single Sparc 20 and utilizes separate file systems on the database server to complete the AMHS functionality. The final configuration uses only the Sparc 1000 or 2000 data server with no dedicated Sparc 20s. Instead, the entire AMHS functionality resides on the database server. The next device in the AMHS suite is the Standard Automated Terminal (SAT), also sometimes referred to as a Secure AUTODIN Terminal (SAT), which contains a specialized communications card for interfacing with the AUTODIN message system. The SAT computer is an Intel 486 based computer operating with the Microsoft Disk Operating System (MS DOS). The next component in the AMHS suite is the cryptographic devices feeding data to the SAT. A large variety of cryptographic devices are used with each being site specific. The next device in the AMHS suite is one of seven different

components (AMME, AFAMPE, LDMX, MDT, ASC, CSP, and AGMS) which are an integral part of the AUTODIN feed to ensure 100% message delivery. Finally, there is a 4800 bits per second (bps) AUTODIN circuit feed. There are a wide variety of AMHS configurations. Each configuration must undergo certification testing by Defense Message System (DMS) certified testers. One stipulation of AMHS certification is that the GCCS LAN, all remote LANs, all backside LANs, all remote dial-in subscribers, and all dedicated circuit subscribers must be protected at the classification level of the AUTODIN feed, otherwise certification will be denied at that GCCS site. Once DMS has fielded a classified version of their message processing software the AMHS and AUTODIN capabilities in GCCS will be replaced.

The GCCS premise router is part of the GCCS site's LAN infrastructure. This represents the gateway out to the SIPRNET WAN or to one of the other major S/A or CINC WANs supporting GCCS. The majority of GCCS premise routers in use are manufactured by Cisco. Some of the models used at the GCCS sites are the Cisco 3000s, the AGS+s, 7000s, and the 7010s. The initial premise routers were supplied by DISA, but they are owned and operated by the individual GCCS sites. As such, it is highly possible that some existing premise routers will be swapped out in the future by some GCCS sites to install a larger capacity router to accommodate their specific mission needs. This is especially true where the GCCS site has a large campus environment (many buildings linked together by routers or bridges) to support. Some sites have already replaced initial premise routers with a different premise router that has greater capability. Replacement routers used by the sites will not necessarily be from the Cisco product line; however, the replacement routers must be compatible with the existing infrastructure.

The next device is the communications server (CS) which is part of the site's LAN infrastructure. The devices initially being provided by DISA but owned and operated by the GCCS sites are the Cisco 2511-CSs. These CSs have two serial ports, one Ethernet port, and 16 asynchronous dial-in ports. The CSs will serve three types of users. The first are users who dial into the GCCS site using a Secure Telephone Unit - III (STU-III) to gain access to the GCCS infrastructure. The second set of users are those who are connected to the GCCS site via low speed dedicated multiplexer circuits. The third user set will be GMC personnel accessing the site via dial-in to assist the site in troubleshooting catastrophic WAN failures. Through the dial-in access, GMC personnel can access the log files of the smart agents to help determine what type of failure occurred at the site. Authentication and access control must be performed at the CS location. Authentication control for CS users will be performed by separate accounts and passwords required by the CS operating software. Access control will be by the STU-III devices or link encryptors. The CS is considered an access point to the general DoD secret-level LAN/WAN infrastructure and must be protected as such. Appendix D contains additional information concerning the CSs being deployed on the GCCS.

Figure 11 shows the various users of a GCCS CS. Besides the CS functioning as a terminal server, the CS is also a full-blown router. It is recommended when sites submit Request For Service (RFS) paperwork to get dual homing to the SIPRNET or other supporting S/A and CINC WANs they use the 2511-CSs as the termination point at their sites. This way if the circuit between the premise router and the WAN fails the circuit between the 2511-CS and the WAN should still be up. For the

DISN, DISA has made a pricing adjustment for sites dual homing to the SIPRNET. The second circuit of equal or less bandwidth of the first circuit is at a 50% cost discount. During submission of the RFS for the second circuit it is important to state the request is for a second circuit and give the information regarding the first circuit. Diverse routing should also be specified.

The STU-III devices connected to the CSs must be new generation STU-IIIs to accommodate the bandwidth requirements of the GCCS applications. It is recommended that the GCCS sites use the AT&T Model 1910 STU-III or equivalent. This particular device has a 14.4 kbps modem engine and obtains throughput speeds of 38.4 kbps using internally supplied compression algorithms. Built in error correction algorithms should also be activated to overcome poor quality telephone lines. Access control will be provided by the Secure Access Control System (SACS) which is part of the AT&T Model 1910 STU-III operating software. The SACS feature operates on an Access Control List (ACL) feature for authenticating valid STU-III connections. It is the responsibility of the GCCS site to provide STU-IIIs and telephone lines to support their dial-in requirements.

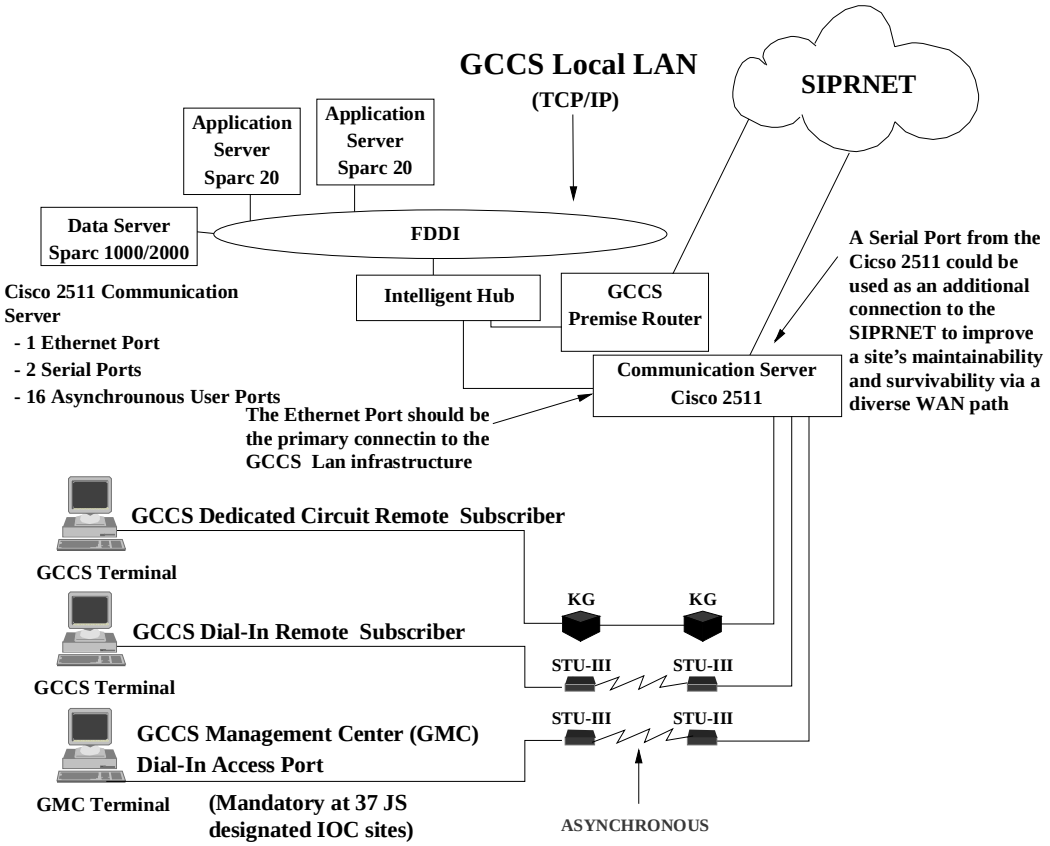


Figure 11 Communication Server Subscriber Types

The next set of devices are the multiplexers and cryptographic equipment used to support the dedicated circuit remote subscribers. This group of users are carryovers from the slow speed

dedicated connections that existed within the WWMCCS community. A majority of these connections were 2.4 and 4.8 kbps in the WWMCCS environment. The vast majority of GCCS applications will not run over circuits this slow. A minimum speed of 32 kbps is recommended for dedicated circuits in the GCCS environment. However, actual experience is showing this may be too slow for some applications in which case 56 kbps would be a more optimum circuit speed. It may be cost effective for remote GCCS users to migrate from dedicated multiplexer circuit basis to a dial-in basis using STU-III technology provided their mission needs can still be meet.

The next item to be discussed is the Fiber Distributed Data Interface (FDDI). This is high speed LAN technology used to interconnect all of the major components of the GCCS site. This includes the data and application servers, and the intelligent hubs. In some cases the premise router may be connected to the FDDI ring instead of being connected to the intelligent hub as shown in Figure 10. DISA provided the FDDI equipment to the initial GCCS sites.

The next group of devices are the intelligent hubs. These are LAN infrastructure devices that allow the FDDI LAN to be connected to the site's normal Ethernet LANs. The intelligent hubs provide the translation function of the LAN speeds and protocols. It's important to note that individual LAN infrastructures will vary greatly from site to site. DISA provided intelligent hubs during the initial equipment deployment. Not all sites elected to install the intelligent hubs provided by DISA. In some cases this was because the sites already had existing capabilities from the same vendor equipment. In other cases it was because the site had a different vendor's equipment installed that satisfied the need. Finally, some sites decided to delay the installation to a future date in time.

The next group of devices are the backside routers and bridges. These will vary from site to site based on the site's complexity. In most cases a GCCS site will not exist within a single building or facility nor contain a single LAN segment. It is highly likely there will be multiple buildings within a close geographical area to form a campus environment. This campus environment would consist of a group of individual LANs interconnected by additional routers or bridges to form the site. The additional routers or bridges are not limited to interconnecting those sites within close geographical proximity. They could also be used to tie in GCCS Remote LANs that are separated by large distances. The existence of these campus environments and GCCS Remote LANs is one of the primary, driving factors for performing network management within the GCCS environment. The performance of the LAN infrastructures in the client-server environment will be more critical than that of the WAN overall performance.

The final group of devices are the clients, the actual users of the GCCS software. The users represent the presentation tier of the three-tier software model. The hardware platforms used by the clients can vary greatly. The GCCS places a strong emphasis on software and not on a hardware dependency. The GCCS software is being developed to operate on the Sun Solaris 2.3 or the Hewlett Packard (HP) HP-UP-9.0.7 operating systems. Other operating systems will be added as the DII COE and GCCS software matures. To run the GCCS suite of software the hardware platform must be able to support one of these operating systems. However, it must be strongly emphasized that this is not the only way for GCCS clients to exist. A hardware platform that uses a different, noncompliant,

operating system can still be used as a GCCS client. This client could run a standard XWindows client application software package to reach a GCCS application server running an Xwindows server application. It would then have all the functionality of the current Sun or HP based clients. Clients identified so far on the GCCS are Sun Sparc 5s, Sun Sparc 10s, Sun Sparc 20s, TAC-3s, TAC-4s, Macintosh IIfxs (also referred to as HoneyMacs or WIS workstations), and a variety of MS DOS based platforms. The hard disk and RAM requirements of each platform depends on what the user wants to operate on that particular hardware platform. If the workstation functions strictly as an XTerminal device, the hardware requirements are not as great as a workstation running GCCS applications resident in that platform. Another point worth noting is that few of the GCCS applications exist in Macintosh IIfxs or MS-DOS operating systems. The hardware requirements of GCCS client workstations are left to the discretion of the GCCS sites based on their mission needs. Recommended minimum hard disk and RAM sizes can be obtained by contacting the DISA Chief GCCS Engineer.

A large majority of the initial GCCS equipment was procured by DISA at the direction of the Joint Staff. Funding for future hardware procurement is the responsibility of the S/As and CINCs. DISA will fund only for DISA specific sites (NMCC, ANMCC, GMCs, and OSF).

3.2.3 Perspective View

The GCCS architecture may be viewed from an organizational or a technical perspective. The organizational perspective focuses upon the communities which use and support the GCCS. The technical perspective focuses upon the three-tier client-server software structure, hardware, and LAN/WAN technologies used within the GCCS. The genesis of these perspectives is in the interpretation of DoD policy and mission statements and the nature of existing and planned technical initiatives. For example, policy and mission require cooperation among assigned forces in a Combined/Joint Task Force (C/JTF), thus leading to the organizational perspective. The GCCS sites derive their physical relationship from the interconnection provided by the DISN SIPRNET WAN and the supporting S/A and CINC WANs leading to the technical perspective. Both perspectives are explained in greater detail below.

3.2.3.1 Organizational Perspective

The communities using the GCCS are the NCA, CINCs, Services, Components, JTFs, and its assigned Service Components. Additionally, DII components that could support the GCCS in the future are the Defense Megacenters (DMCs), consolidated management centers, base-level communications, and the DISN. A complex logical relationship will exist with the GCCS community as well as among those external communities and information sources; such as national assets from weather and emergency relief agencies and international military agencies like the North Atlantic Treaty Organization (NATO). Effective support of this relationship depends upon extensive

technical support from DII components which among themselves comprise an extensive inter-component relationship.

An example of this complex relationship within the DII can be seen by referring to Figure 12. The Defense Megacenters (DMCs) may contain "reachback" information repositories at the secret classification level that a GCCS user needs to access. The information repositories are maintained by the DISA System Management Center (SMC) responding to the direction of a DISN RCC operated by DISA. A user at one GCCS site located on a post, campus, or station may wish to correlate reachback information from their location with reachback information at one of the Megacenters. The information repositories at the Megacenters are maintained by the DISA DISN portion of the DII and are outside the normal boundaries of the GMC for the GCCS. Should system anomalies occur during the user's correlation process, the GCCS site may need to rely upon their GCCS System Administrator, working with the GMC-Pentagon, to resolve the problem with a peer administrator at the SMC. The following figure helps to show the DII interrelationships.

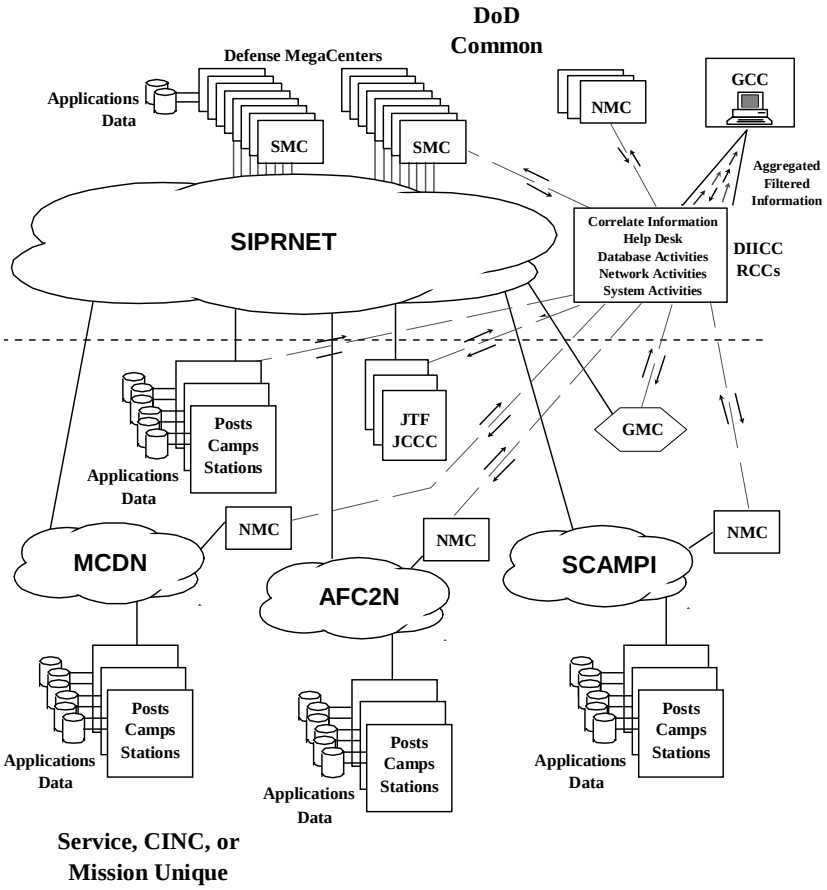


Figure 12 DII Component Interrelationship

3.2.3.2 Technical Perspective

The three-tier client-server structure is the starting point of the GCCS architecture's technical

perspective. This structure coupled with the hardware and LAN/WAN technology used gives a clear technical picture of the GCCS. The technical perspective may be applied to the organizational perspective above to show how different organizations will physically interconnect. The GCCS sites each operate their own LANs, an example of which was shown in Figure 10 previously. These LANs are interconnected by the SIPRNET WAN of the DISN or the other S/A and CINC WANs. A drawing would show the complex network architecture that links all of the GCCS community together.

3.3 GCCS Relationship to the DII and DISN

The DII is composed of the information infrastructure for the deployed C/JTF (headquarters and forward components), the sustaining base (command and finance centers, as well as other similar facilities), and the DII utility (Megacenters, DSN, DSCS, DISN, etc.). The GCCS is a set of shared command and control applications and operates as a part of the secret level DII to provide the information resources required by warfighters to accomplish their C2 missions. A key part of this definition is that the GCCS is a part of all aspects of the DII and must be DII compliant. Accordingly, the GCCS must be supported by a management center independent yet the management center is integrated with the DIICC consolidation concepts. In other words, the GCCS must develop an LCC function to support the GCCS community while at the same time exchanging management data with the DII/DISN GCC and RCCs. This integration includes both non-GCCS information systems and the DISN, and it imposes a reciprocal responsibility upon those entities to ensure support for the GCCS in accordance with Joint Staff policy and derived requirements. This conceptual integration of the GCCS into an integrated management concept will lead to the eventual geographic consolidation of GCCS GMC functions, more effective integration of the life-cycle aspects of GCCS information systems development, and support to the Joint Staff commensurate with changing technical and political realities.

Special attention must also be directed to the relationship of the GCCS to the DISN. The GMC will manage the overall status and operations of the GCCS but not the SIPRNET which is part of the DISN. This implies that the GMC is more than a "network" operations center. It also has a responsibility for the "information systems" operations. To maintain both the "network" and "information systems" operationally, the GMC will continue to rely upon the DISN for information. The GMC relies on the SIPRNET RCCs for the GCCS just like the WIN NOC currently relies upon the DSNET2 Operations Center for the WWMCCS. This interaction of management entities is also in concert with integrated management concepts which distinguish between network and system management and the inter-dependency relationship of each. This same special attention must be directed to the other S/A and CINC supporting WANs. A strong interaction will be required between their management centers and the GMC. Section 3.4.5 discusses in more detail the LCCs that will be used to manage the GCCS.

The GMC is manned by DISA/WESTHEM/ Joint Staff Support Center (JSSC) personnel. The GCC/RCCs are manned by DISA/D3 personnel. They are two different organizations within DISA tasked with different areas of responsibility. One of the tasks of DISA/D3 is to maintain the global

networks DISA has responsibility for whereas the DISA/WESTHEM JSSC people are responsible for providing direct support to the Joint Staff on DISA sponsored/owned systems installed at the Pentagon. Some mistakenly think the DISA/WESTHEM departments are part of DISA/D3. This is not the case and both organizations are to be treated as separate entities.

3.4 GCCS Management Architecture and Functions

The GCCS system and network management architecture is influenced by the internal GCCS environment and the external organizations on which the GCCS relies. From a technical viewpoint this can be looked at as either the system environment or the network environment. The following identifies the GCCS system and network environments that will influence the structure of the GMC.

The system environment characterizes the applications within the GCCS as distributed. This implies the applications may be located in geographically diverse areas, control of the application's three-tiered components may not be under one administration, or the methods of communications access may vary across the system. The applications are collaborative in the sense that a diverse spectrum of users will have the ability to interact within a number of the different applications via multiple user sessions. This collaborative interaction will require the GMC to be able to interact with its peer management organizations in order to maintain the maximum possible efficiency of the GCCS applications. The system environment also includes the hardware platforms in one sense. The capabilities of each platform will dictate the efficiency of how the software applications behave. For example, a Sparc 5 with 128 MB of RAM will run an application differently than a Sparc 5 that only has 64 MB of RAM.

The GCCS system contains two security levels as previously identified with the majority of operations being conducted at the system high secret level. The security policy for the GCCS considers a number of threats and external and internal system interfaces. The security policy will consider the interface requirements of all GCCS applications as they evolve. The system and network management applications in the GMC, though not mission-oriented, must also comply with the security policy.

The GCCS operates in three modes. The first is On-Line. This is the normal mode of operation where the GCCS is on-line capable of performing its operational mission. The second is a Maintenance mode. In this mode portions of the hardware or software at a GCCS site will be off-line. This may be due to a hard equipment failure or for routine maintenance. For example, a software application may be taken off-line to replace it with a newer version. The third mode of operation is Exercise. In this mode a portion of the GCCS may be operated with separate databases using simulated inputs. This could be for war gaming purposes or for testing new functionalities for the GCCS. It is important to understand these modes of operation are not mutually exclusive. In fact, normal day-to-day operations will probably find all three operating modes existing at the same time on different portions of the GCCS. The different modes will be distinguished by administrative features or architectural boundaries.

The network environment characteristics rely extensively on the DII DISN and the S/A and CINC WANs for its direct support of the GCCS. Access to the DISN and the S/A and CINC WAN communications infrastructures will be from any location on the globe through all possible means. The GCCS requires a survivable, reliable, and available global network which can accommodate future video as well as current data requirements. The supporting network must be able to sustain a wide traffic load variation in both peacetime and wartime. Additionally, the GCCS is only one of the many communities on the DISN SIPRNET and the S/A and CINC WANs. As such, the C2 wartime bandwidth requirements must be factored in to the design of each of the WANs. The GCCS contains within itself a communications infrastructure of routers and LANs managed by the CINCs and S/As. In addition to the conventional sense of "network", the GCCS is a virtual network of interoperating information system servers operating across the DISN and S/A and CINC WANs all monitored by the GMC and managed day-to-day by the individual sites.

Additionally, one must look to the DISN network management structure to understand the task the GMC must perform. From Figure 2 it can be shown the GMC must perform the function of the LCC for the GCCS subscriber community. Besides this “networking” role the GMC must also perform the additional system management functions required by the GCCS described in the following sections.

3.4.1 GCCS Management Center (GMC) Definition

The elements necessary for defining the GMC are now established. The generic term “GMC” will represent the management function solely responsible for the joint operation of the GCCS. However, while the GMC is responsible for managing the GCCS, different areas of responsibility will be delegated to other subordinate offices for more efficient operations. In essence, the GMC will be a collection of offices functioning under a single management umbrella. The various functions performed by these offices will be identified later.

This collection of offices will use a combination of COTS and GOTS system and network management applications to continually monitor the health of the GCCS. The GMC will function as a specialized or Primary LCC for the GCCS community concerning system and network management. The GMC will be the office with primary responsibility for all management aspects of the GCCS. This management oversight must operate in accordance with all DII system and network management concepts. This includes management of all joint applications operating in the GCCS environment. S/As or CINC unique applications will adhere to the policy set forth by the OPR for that particular S/A or CINC application. In time, all S/A and CINC applications will be required to migrate to the DII system management concepts.

The existing WWMCCS network and system management structures are not well suited for the GCCS environment since it lacks a fully integrated chain of command. Several offices were responsible for system management activities on the WWMCCS while others were responsible for network management activities. These offices were not always under the same organization or leadership. The complexity of the GCCS will require a transition from the WWMCCS way of doing

business to the GCCS network and system management structure. This transition will take time to accomplish. Included in the following sections are two diagrams that will help show the initial and target architecture of the GMC. It is important to understand that GMC IOC is independent of the GCCS IOC.

Figure 13 shows the initial configuration of the GMC. The GMC is made up of three main locations: the GMC-Pentagon, the GMC-Site R, and the GMC-OSF. The GMC-Pentagon is the office of primary responsibility and all other GMC offices are subordinate to this office with the exception of the current TS3 program. The TS3 portion of the GCCS will remain under the WWMCCS management infrastructure until it is migrated to the GCCS(T) solution. The GMC-Pentagon will receive direction from the GCCS Director (GCCS DIR (defined in sections 3.4.8 and 4.2.2)) on all matters concerning operations on the GCCS and will disseminate this information to the other GMC offices. In addition to the three main locations there are two major supporting functions to the GMC-Pentagon. The first is the GMC-JOPES which is comprised of the existing DISA/WESTHEM/JSSC offices supporting JOPES. The GMC-JOPES will be responsible for system management of the JOPES applications on the GCCS initially using the GCCS System Services application. The GMC-JOPES office will no longer be a separate entity in the final configuration. It will be combined with the GMC-Pentagon into a single entity performing operational management of the GCCS. This transition has occurred and the GMC-JOPES no longer exists. The other supporting office is the OSF Hotline which was initially brought online as the trouble call location at the DISA OSF facility. The physical location and operational control of the GMC-HelpDesk has moved from the GMC-OSF facility to the GMC-Pentagon as shown in the final configuration. The relationship of the GMC offices in the initial configuration is shown below.

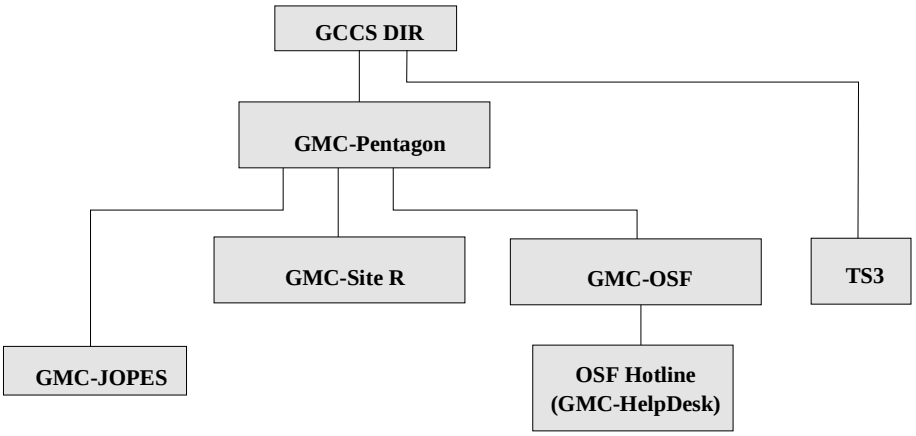


Figure 13 GMC Components at Initial Operating Capability

Figure 14 shows the final configuration of the GMC management structure. Several changes exist between the IOC and FOC structures. The GMC-JOPES is now included in the GMC-Pentagon. The GMC-HelpDesk moved from the OSF Hotline location and became part of the GMC-Pentagon. The final change occurs when TS3 (top secret portion of the GCCS) is migrated to its final configuration of the GCCS(T). The GCCS(T) will be managed by the GMC and the remaining portion of the WWMCCS management infrastructure can be terminated. Each of the three main GMC locations will have top secret system and network management capabilities to support the GCCS(T).

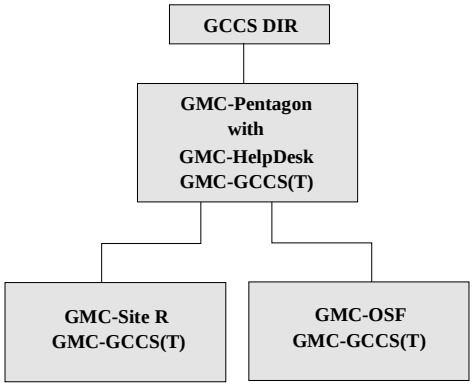


Figure 14 GMC Components at Final Operating Capability

3.4.2 Mission versus Geographic Perspective, DII Considerations

Management of the GCCS can be viewed from two perspectives. A functional requirements specification for the DII IMS implies that Megacenter SMCs are being designed with a geographical perspective. The functional requirements document refers to moving the Megacenter's SMC function to the integrated management hub which is described in geographic terms. This transition corresponds to the DISN goal network management architecture of consolidated management functions. The DISN architecture also distinguishes itself as providing a DISN view from the user's mission perspective. The GCCS requires both a geographic perspective based on the existing DISN and S/A and CINC WAN structures and a mission perspective based upon the collaborative nature of GCCS information systems which cross CINC and S/A boundaries. In this fashion, any future DIICC integrated centers supporting the GCCS must provide a geographic orientation using DISN management concept constructs and a mission orientation using GMC (ie, GCCS SMC) constructs.

3.4.3 GCCS Management Center Functions

The GCCS Management Center is comprised of three Functional Components. These are Planning and Engineering, Management, and Operations. The functional components and their major categories are summarized in the tables below.

Planning and Engineering		
Administration - Policy - Procedures - Training	Planning - Capacity - Services - Rates/Billing - Finance	Engineering - Design - Modeling - Optimization - Operational Evaluation

Table 2 Planning and Engineering Functional Component and Categories

Management

Configuration Mgmt - Network Configuration - System Hardware Configuration - System Software Configuration - Naming and Addressing - Inventory Control - Smart Agent Deployment	Security Mgmt - Objectives -- Accountability -- Integrity -- Availability -- Confidentiality - Support Services - Assurances -- Certification -- Accreditation	Provisioning - Hardware - Software - Acquisition - Integration - Testing - Acceptance	Logistics - Maintenance - Supply

Table 3 Management Functional Component and Categories

Operations	
Monitor and Control - Synchronization of databases - Operational Evaluation and Status - Technical Support	Help Desk - System Management - Network Management - Application and Functional Experts - Support Centers

Table 4 Operations Functional Component and Categories

3.4.4 International Standards Organization (ISO) Functional Management Areas

Each of the three GCCS functional components described in the previous section performs its functions through one or more of the International Standards Organization's (ISO) Functional Management Areas (FMA). The five FMAs are Fault, Configuration, Accounting, Performance and Security Management. The ISO model for management applies the FMAs concepts to both network and system management. The GMC will employ a system management perspective for the overall GCCS and a network management perspective for the individual GCCS sites and their campus components. Network management of the DISN SIPRNET WAN and the S/A and CINC WANs will

be performed by the DII components responsible for these actions.

The remainder of section 3.4.4 will discuss functions of the GMC using the ISO FMA. These FMAs were the building blocks of tables 2, 3, and 4 above. The FMAs permeate the GMC Functional Components and will be used extensively for defining various management functions needed for the GCCS.

3.4.4.1 Configuration Management (CM)

The GMC will provide the configuration management functions to identify, exercise control over, and to collect and provide data on the GCCS for the purposes of status, accounting, and auditing. A summary of CM functions which the GMC will be involved with are; Network Configuration, System Hardware Configuration, System Software Configuration, Naming and Addressing, Inventory Control, and Smart Agent Deployment. Within the GCCS the term Network Configuration includes the network devices at the primary GCCS sites, any associated campus network devices, and any remote sites devices feeding into the primary GCCS sites. This level of detail will provide a concise picture of the GCCS "virtual network" configuration. The GMC will incorporate network configurations to the extent required to support the GMC Functional Components and the other ISO FMAs. The GMC will acquire and maintain inventories of the GCCS hardware to include the premise routers, the communications servers, the data and application (primary, secondary, OPS/INTEL, and MAP) servers, the Automated Message Handling System (AMHS), the intelligent hubs, and other pertinent equipment. A software configuration inventory will be maintained for the COE, mission applications, operational support applications (network management, trouble ticket, and directory services), management support applications (modeling tools, data analysis tools), and associated databases. The final inventory will be a collection of data providing names and addresses of various Points of Contact (POCs), trouble reports, performance reports, change management logs, tariffs, network topologies, pertinent service level agreements, and provisioning orders. Where possible this data collection will be gathered using smart agents resident on each platform with automatic configuration reporting back to the GMC-Pentagon.

These inventories may be used by the other FMAs within the GMC. For example, fault management may require an automated way of manipulating the current server topology when server interconnection or server hardware failures occur. The resolution may require the fault manager to reconfigure the server network interconnection and then update the server topology. Specific CM polices and procedures are still being worked in the draft Joint Staff policy on GCCS CM. Additional information can be found in the draft CJCSI 6722.01, *GCCS Configuration Management Policy* document.

3.4.4.2 Security Management (SM)

The scope of GCCS Security Management (GSM) is derived from the GCCS Security Policy, CJCSI 6731.01 and from national security policy. The GSM will safeguard against various threats such as

unauthorized information access, expanding authorized access without appropriate authorization, information destruction, denial of service, etc. The GSM must also operate in concert with the security management procedures of those systems supporting the GCCS, such as the DISN SIPRNET WAN, the S/A and CINC WANs, and local site facilities, which can be the source of external threats. The DoD Goal Security Architecture (DGSA) further defines the security management environment in terms of "multiple information domains" each of which may be subject to different security policies. This implies that the GSM must evolve as the threats evolve. The threat definition process will require security personnel to coordinate with the intelligence community and with the Center for Information System Security Counter-Measures Department for vulnerability analysis, penetration detection, and assistance in reaction to intrusions and attacks. In addition to ensuring protection against threat, GSM will not cause undue burden upon authorized users in their requirements for information and service access. The complete GSM activity will include, but is not limited to, the following:

- Developing a threat analysis for the GCCS
- Performing an ongoing evaluation of security services, devices (C2 guards), and management procedures
- Operating alarming, logging, and reporting systems
- Protecting the system and network management systems themselves
- Safeguarding/administering other areas such as authentication, access control, encryption, and audit trails. This includes ensuring proper security measures are taken on all network devices (routers, intelligent hubs, 2511-CSs, etc.)
- Controlling and monitoring the mechanisms which exist to protect network and system resources and user information

3.4.4.3 Fault Management (FM)

Central to the GCCS fault management environment is the need for a collaborative response for the detection, isolation, and repair of faults within the GCCS. The GCCS environment includes a global network hierarchy (DISN SIPRNET WAN, S/A and CINC WANs, GCCS sites, and remote GCCS users), two general domains (strategic and deployed tactical (JTF) resources), non-GCCS users in at least the strategic network domain, and multiple NMCs/SMCs which may operate their own help desks. For FM to function effectively in such a complex environment, the GMC requires tools to interpret various Management Information Base (MIB) formats, present the collected information in ways adapted to the environment, and share that presentation with peers in associated NMCs/SMCs. One of the GCCS design goals is that it shall not contain any "single points of failure", often referred to as choke points, throughout the system. In time this will occur; however, the current GCCS is full of single points of failure in the communications environment because sites have failed to submit RFS paperwork for dual homing (see Figure 11). Less than 5% of the GCCS sites are dual homed to supporting WAN entities. Those sites that are single homed need to submit the RFS for the second circuits. When possible they should use the 2511-CS or a different premise router for complete redundancy. Once the robustness and diversity has been achieved in the communications environment, the GMC must be sensitive to events occurring outside the control of the GMC which

would compromise this goal. For example, if a SIPRNET or S/A or CINC WAN router fails, what GCCS sites that where dual-homed are now single threaded connectivity wise?

Various FM tools are required to support the FM functions. The first is a network status supervision tool to receive the status of the SIPRNET from the DII GCC (or designated DII RCC) or the status of S/A and CINC WANs from their management centers, to monitor/control GCCS site networks as necessary, and to monitor/control certain remote GCCS locations networks. A dynamic trouble tracking system is required to handle primarily information system faults, but also to deal with network faults resulting in GCCS faults. In the case of certain WAN faults, the GMC will only monitor the fault resolution progress being performed and tracked separately by the DISN RCCs or the appropriate S/A or CINC WAN management entity. FM trouble tracking will be sensitive automatically to the resolution of error conditions to the extent possible and will generate reports for planning and engineering. A backup and reconfiguration tool set is required to ensure the currency of data and applications, and to support the three GCCS modes of operation (on-line, maintenance, exercise). A diagnostic and repair facilities tool is needed to interpret faults, to determine the most appropriate resolution, and to apply the correction to the operational system. This tool may be the most organizationally intense due to the criticality of certain situations. It will require the fullest implementation of collaborative tools and procedures possible for the GCCS. And finally, an end-to-end testing tool to ensure basic functionality in a controlled environment prior to deployment on the GCCS will be required. This tool can be used upon initial deployment in unique operational environments and to provide basic help in isolating operational problems in the customer's environment.

Where possible FM information will be gathered using smart agents resident on various hardware platform or LAN segments. These agents will be set up with automatic fault reporting back to the GMC-Pentagon. At the same time these FM agents can also be configured with the IP address/Domain Name Service (DNS) name of the site's or organization's management station so they can also receive the FM data.

3.4.4.4 Performance Management (PM)

Monitoring and controlling the quality of network communications and the information systems are the primary thrust of PM. It involves the processes of monitoring and analyzing, tuning and controlling, and reporting on network and information system components to include the system as a whole. The monitoring and analyzing functions include establishing the monitoring environment, the performance indicators, and the generation of appropriate reports. Tuning and controlling functions include activation of controls in order to fine tune the performance of the network and information systems. The recognition and diagnosis of performance deficiencies are considered fundamental requirements of PM. Good PM procedures and practices coupled with properly enabled monitoring and reporting tools will identify problem areas before hard failures occur. By taking prompt action on PM identified problems, major outages and mission impacts can be avoided. The PM reports generated can include reports on performance monitoring, tuning, tracking, and trend analysis.

Preliminary work identified the network and system management complexities involved with the migration from a WWMCCS mainframe to a GCCS client-server environment. Generally, mainframe environments manage resources centrally while client-server environments include domains of management. The management of domains affects all management functional areas, but it affects the PM area the most because it integrates the actions of heterogeneous networks and information systems. The other management functional areas can serve individual components more independently. Ideally, PM will integrate its view in real time so that operations may more quickly react to performance issues. Thus, PM is perhaps the most complex management functional area and must be given extreme attention as the GMC is implemented.

The requirements for PM relate to the transmission circuits, circuit nodes, Inter-Router Trunks (IRTs) of the WANs, WAN routers, GCCS premise routers, LANs, and mainframe and client-server information systems. Transmission circuit, circuit node, WAN IRT, and WAN router performance are outside the scope of the GMC except that a link or router status (up or down) must be available through the SIPRNET RCCs and the S/A and CINC WAN management centers. The GMC will, in its initial stages, be sensitive to node performance only as it relates to link status. The criteria for GCCS router and LAN performance requirements are based upon packet throughput, end-to-end delay, data integrity, probability of misdelivery, network availability, and continuity of service. The criteria generally will be established at levels supported by current commercial availability. Continual evaluation of these criteria against required traffic levels is required since the GCCS information systems may drive the communications infrastructure to available limits. Additionally, traffic level criteria must allow tolerance within the network infrastructure for the increased communications requirements during a war time or crisis situation. A PM criteria based on peacetime requirements will be inadequate when the system is needed for a national crisis.

Where possible PM information will be gathered using smart agents resident on various hardware platform or LAN segments. These agents will be set up with automatic fault reporting back to the GMC-Pentagon. At the same time these PM agents can also be configured with the IP address/DNS name of the site's or organization's management station so they can also receive the PM data.

In summary, PM will be an ongoing activity of defining performance indicators and establishing operating standards to balance mission requirements against information and network system capabilities. PM will produce threshold and exception reports for subsequent analysis and tuning of the systems.

3.4.4.5 Accounting Management (AM)

This area provides the functionality of identifying cost components, establishing charge-back policies, defining charge-back procedures, and defining procedures for processing vendor bills. Typically AM specifies: the usage data to collect, establishment and modification of accounting limits, collection

and storage of usage data, access and storage control of usage data, and report generation. The GCCS does not have a requirement to use charge-back procedures since C2 systems are appropriated and do not have to recover costs. The extent of AM involvement by the GCCS is limited to the GCCS sites paying for their SIPRNET access circuits, S/A WAN access circuits, and any other communications cost incurred from the DISN or other sources. In simpler terms, as long as GCCS sites pay their monthly connectivity bill to the WAN entities, we are customers in good standing. Some of the AM functionality would be beneficial to the GCCS community for determining costs and monetary trend analysis for any future functional economic analysis of the GCCS. How to implement these capabilities needs to be determined before this functionality is incorporated into the final GMC capabilities.

3.4.5 Primary and Secondary LCCs

As explained earlier in section 2.2.1, the DISN uses a three layer model to define the different areas of network management responsibility. The GCC and RCCs of the DISN do not control any subscriber assets owned by the individual S/As connected to the WANs. In the future, one of the DISN services that will be available will be for the RCCs to manage subscriber assets. Again, like the network connectivity this would be on a fee-for-service basis. GCCS may take advantage of these capabilities later on. For now, the GCCS community must manage its own assets and establish LCCs which are the third layer of the DISN hierarchy model.

The GCCS will establish two levels of LCCs within the community. These are referred to as Primary and Secondary LCCs using DII/DISN management terms. The Primary LCCs are the high level management centers that make up the GMC. Their primary purpose is to support the Joint Staff oversight requirements of the GCCS. The GMC locations are manned by DISA personnel. The Secondary LCCs are the system and network (local and CINC unique communications infrastructure) management capabilities for the CINC and S/A GCCS sites. The Secondary LCCs give the individual GCCS sites the day-to-day system and network management responsibility to manage themselves effectively. The Secondary LCCs will be implemented based on guidance and direction from the S/A GCCS PMO according to S/A policy. Management tools for the Secondary LCCs are the responsibility of the S/A GCCS PMOs of that particular organization based on the S/A doctrine for system and network management. The DISA GCCS PMO will provide the smart agents that will be discussed later in the document. Varying degrees of responsibility will be shared between the Primary and Secondary LCCs. These will be further defined in section 4. Figure 15 helps to better define the relationships between the GCC, the RCCs, and the Primary and Secondary LCCs used for the GCCS. Though DISA will man the GMC (Primary LCC) locations it is important for one to understand it is a Joint Staff/J-3 management oversight mission being performed at these locations.

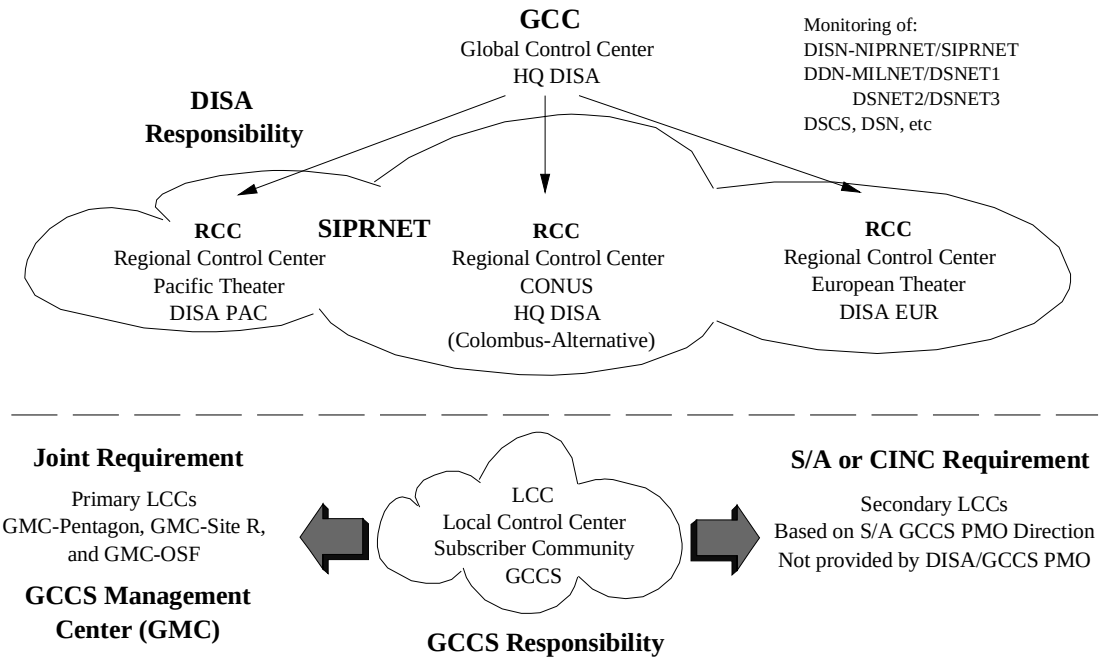


Figure 15 Primary and Secondary LCC Requirements Diagram

3.4.5.1 Primary LCC (GMC) Locations

DISA will establish three Primary LCCs. Collectively these three sites will perform the GMC functions with each site having the capability to perform the entire GMC functions stand alone. The three sites are at the National Military Command Center (NMCC) located in the Pentagon (called the GMC-Pentagon), the Alternate NMCC (ANMCC) located at Site R (called the GMC-Site R), and the DISA Operational Support Facility (OSF) located in Sterling, Virginia (called the GMC-OSF). The GMC-Pentagon and GMC-Site R locations will be operational 24 hours a day, 7 days a week, managing the GCCS though the GMC-Site R location will operate more in a hot standby mode. The GMC-Site R locations will be augmented by GMC-Pentagon personnel during extended outages. The GMC-HelpDesk was initially at the OSF. Operational control of the GMC-HelpDesk passed to the GMC-Pentagon on 6 June, 1996. The GMC-OSF resumed normal business hours of 8 hours a day, 5 days a week. The GMC-OSF will be involved primarily with upgrades and enhancements to the GCCS and not day-to-day operations and management. As such, the GMC-OSF no longer takes GCCS trouble calls from the field. The GMC-Site R operates 24 hours a day, 7 days a week, to ensure the site can assume operational control of our nation's defenses in the event the GMC-Pentagon has been destroyed, rendered inoperative, or is placed off-line for maintenance. Each of

the Primary LCCs will have a secret area to manage the secret high portions of the GCCS and a top secret high area to manage the top secret, TS3 portion of GCCS. The initial requirement for managing TS3 is not as severe nor time sensitive as the secret high portions of the GCCS. This is due largely to the fact the TS3 system is a residual part of the existing WWMCCS and some of the network and system management functionalities from WWMCCS are being maintained to support TS3. TS3 will migrate to a client-server environment using Sun Sparc servers and terminals similar to the secret high GCCS. The future top secret capability of the GCCS is referred to as GCCS (T) and will require extensive system and network management. This document only includes the preliminary infrastructure necessary for managing GCCS(T); an additional CONOPS may be required for GCCS(T).

Figure 16 is a high level representation of the three Primary LCCs for the GCCS. The center of the figure represents the SIPRNET WAN and specifically shows the three SIPRNET backbone routers that support the identified GCCS sites. The GCCS sites are connected either through a serial or Ethernet connection to the SIPRNET WAN. The Primary LCCs will be attached to the LAN at the supporting GCCS site. The Primary LCCs show both the secret and top secret portions of the GMC.

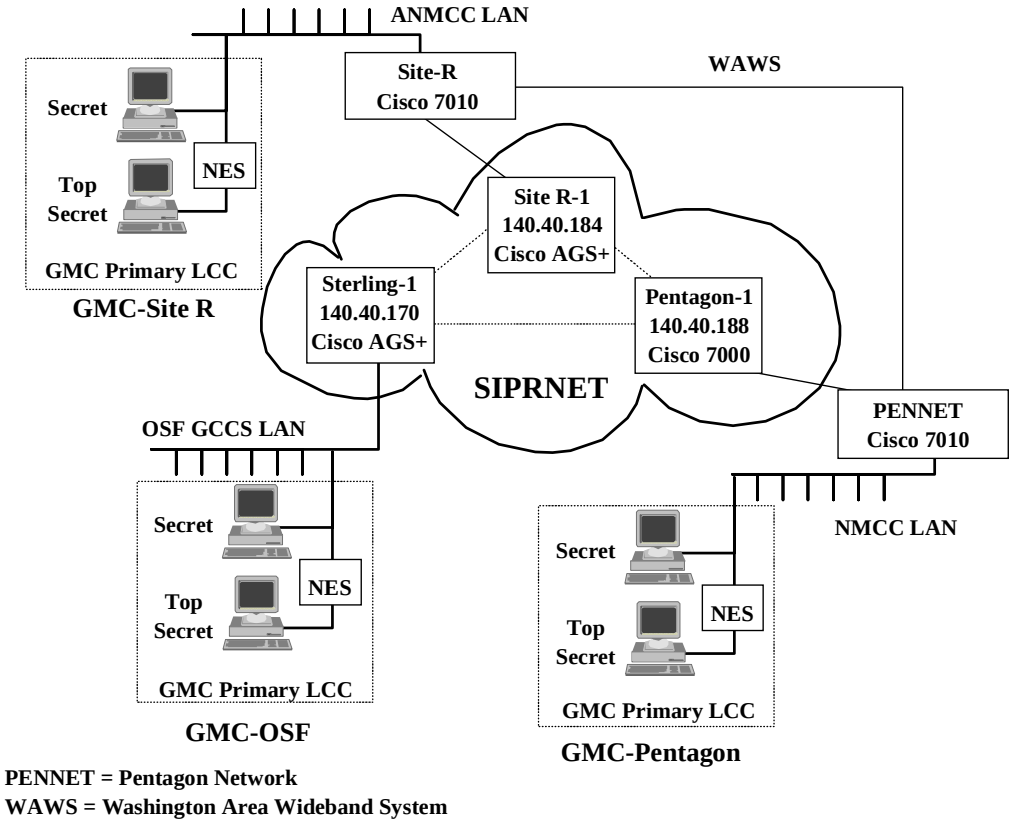


Figure 16 GMC Primary LCC Locations

3.4.5.2 Secondary LCC (CINC & S/A) Locations

The Secondary LCCs are at the CINC and S/A GCCS sites to perform their own day-to-day system and network (local and CINC unique communications infrastructure) management. Several factors complicate the fielding of management capabilities to the CINC and S/As GCCS sites. First, funding levels for GCCS are in a state of flux and still being determined. The initial funds did not exist for purchasing the management software needed for all secondary locations. Next, there are several base level initiatives ongoing within the S/As to consolidate management functions on a base or post. Most notably is the Air Force's Base-Level Network Control Center (BNCC). Under the BNCC program there is a single management entity on a base taking care of all base networks and systems of all classification levels. This management entity will provide management of C2 capabilities, Office Automation, Business Processing Systems, etc., on that base. This will include the GCCS assets thus eliminating the need for a Secondary LCC specifically at that GCCS site. At AF sites implementing BNCCs, Secondary LCCs may need to be established by the CINC and S/A PMOs until the BNCC is ready to assume the Secondary LCC responsibilities for the GCCS. Another factor is the direction the United States Marine Corps (USMC) is taking for managing their sites. The Marine Corps operates a USMC Network Operations Center (24 hours by 7 days a week) at Quantico, VA, which coordinates with each base/major subordinate command (MSC) wide area and local area network managers. This USMC NOC monitors and controls all of the USMC NIPRNET/SIPRNET connections and dedicated long haul routed bandwidth. This greatly reduces the required management functions at specific USMC sites.

Finally, several sites already have some form of system and network management capability in place. These sites are reluctant to change to a different operating concept. The management by exception approach being taken on the GCCS can accommodate sites using different systems. The various SNMP agents being integrated into the GCCS environment can be configured to report events and traps to any type of SNMP based management platform.

The Secondary LCCs give the individual GCCS sites the day-to-day system and network management responsibility to manage themselves. Individual S/A GCCS PMOs, based on dictated S/A policy, describe to their subordinate sites how they will be managed. Because of the above complications, the DISA GCCS PMO will not provide any hardware or software to the GCCS sites for the creation of the Secondary LCCs with the exception of the smart agents which may be required. If needed, the Primary LCCs will try to assist GCCS site personnel in managing the site's GCCS assets until such time as the S/A GCCS PMOs can field the Secondary LCC functionality.

DISA is responsible for the day-to-day operations of the NMCC and ANMCC locations. Because of this mission requirement the GMC-Pentagon will have the additional responsibility of being the Secondary LCC for the DISA sponsored NMCC location. Likewise, the GMC-Site R will serve as the Secondary LCC for the DISA sponsored ANMCC location.

3.4.6 GMC Hardware Architecture

As previously stated, three sites collectively form the GMC. Each site will require workstations for the GMC technicians to perform system and network management. Application servers for the GMC software will also be required. Additionally, the GMC-Pentagon and GMC-Site R locations will require database server space for containing various forms of GMC management data. Initially this data may be stored on the NMCC and ANMCC Sparc 1000s while Oracle licenses are obtained for the GMC servers. The GMC-OSF will operate as a client to the database at the GMC-Pentagon with the GMC-Site R database server acting as a backup. GCCS system and network management data from the GMC-Pentagon database server will be backed up to the GMC-Site R database server. When possible, backups will occur real time between the two management centers. Specific backup procedures will be identified in the *Global Command and Control System (GCCS), System and Network Management, Implementation Plan* which will identify the technical and day-to-day operational requirements for GMC operations.

Figures 17, 18, and 19 show the proposed initial hardware architecture that will be used to support the GMC mission. Shown are the technician workstations, the various GMC applications servers and database servers, and secure telephones required to support the GMC locations. Not shown are the NMCC and ANMCC database servers that may be used temporarily for GMC data storage requirements. These three figures complement the generic sites used in Figure 16. The capabilities shown will be explained in greater detail in the following sections.

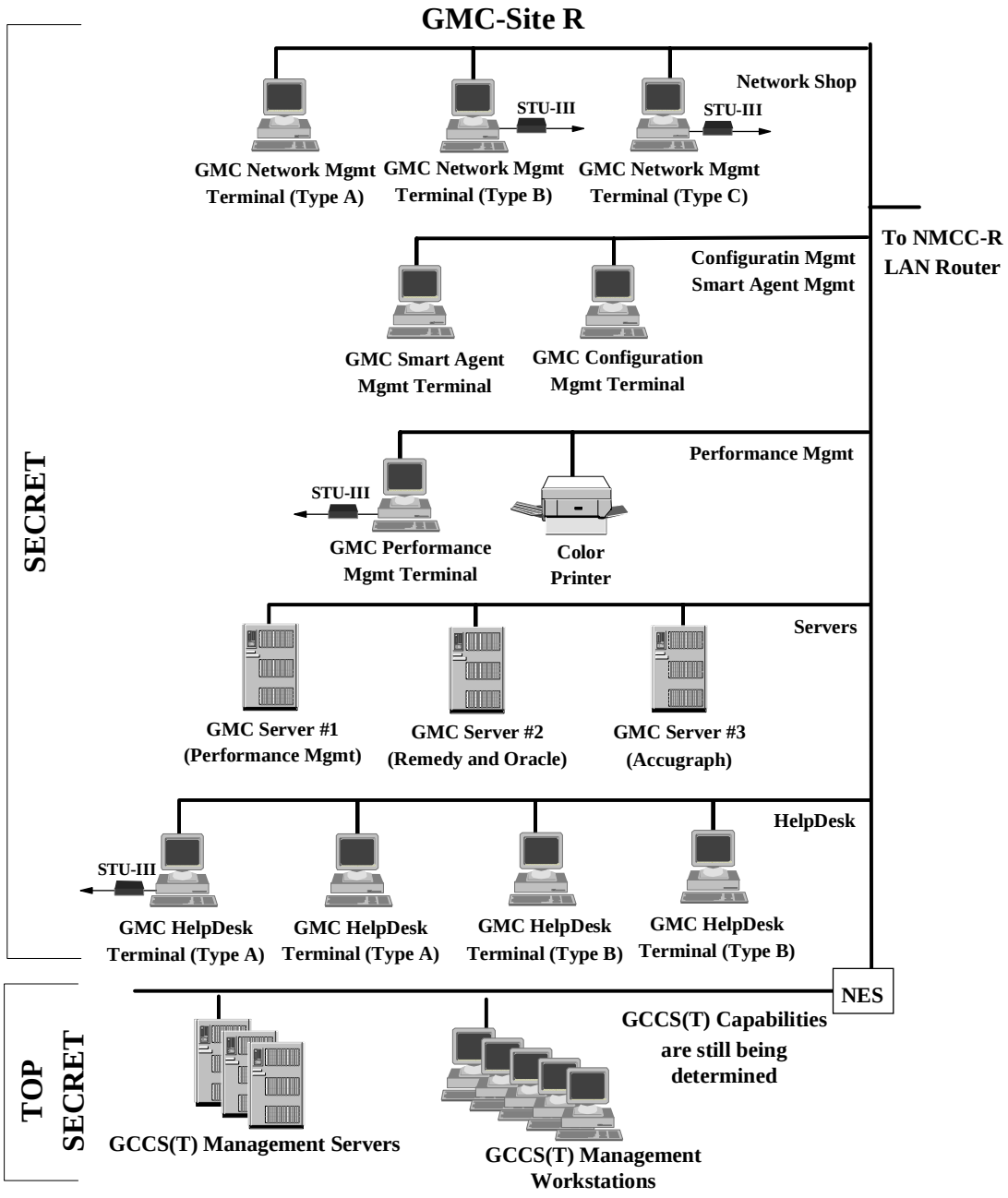


Figure 17 GMC Hardware Architecture for the GMC-Site R

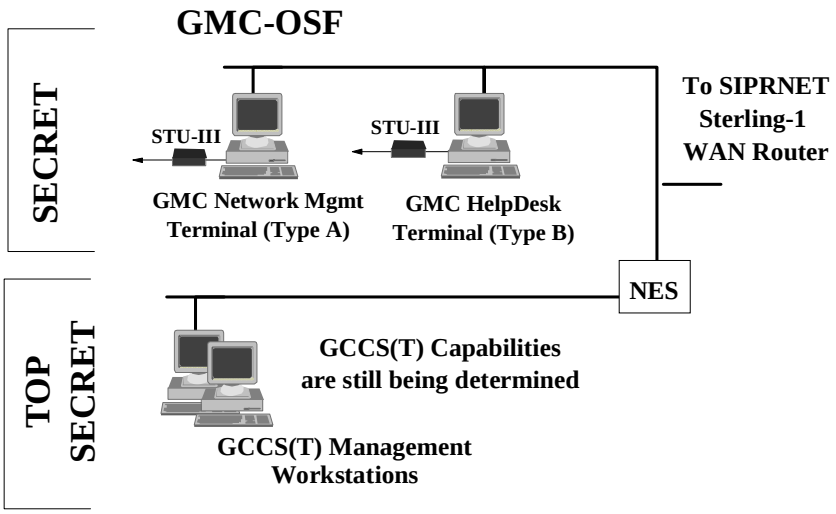


Figure 18 GMC Hardware Architecture for the GMC-OSF

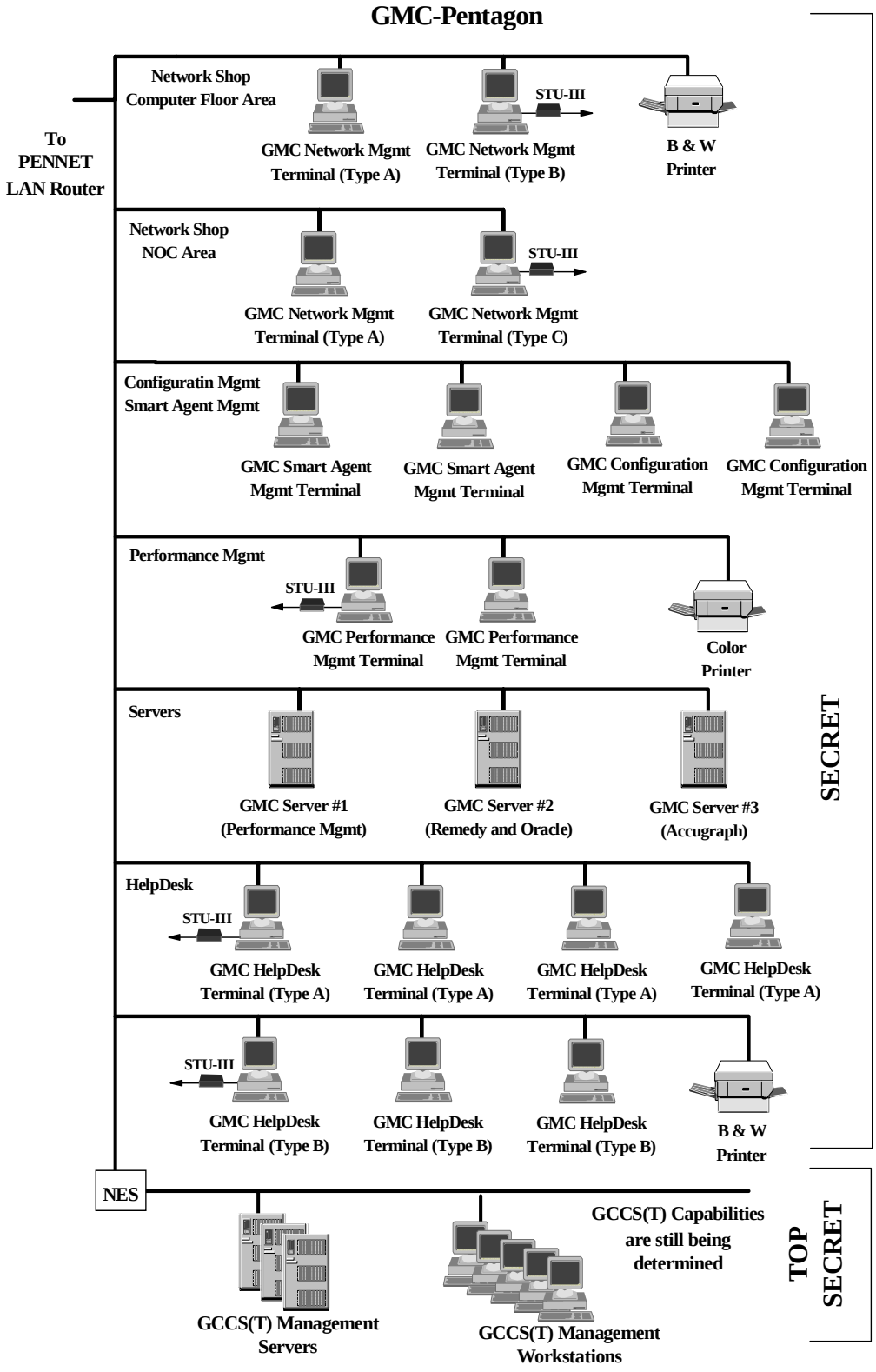


Figure 19 GMC Hardware Architecture for the GMC-Pentagon

3.4.6.1 Secret Level Capabilities

Each of the three GMC locations will require hardware operating at the secret level to perform system and network management. Figures 17, 18, and 19 show the GMC-Pentagon, GMC-Site R, and GMC-OSF hardware architectures. Each of the sites will receive client workstations to be used by the GMC technicians. The client workstations will be spread between the various functions identified in the figures. Additionally the GMC-Pentagon and GMC-Site R will each receive three Sparc 20s that will be the application and database servers for the GMC joint oversight mission. The GMC-OSF will not receive any servers. The GMC-OSF will operate off of the GMC-Pentagon application and database servers. As previously stated the data from the GMC-Pentagon will be backed up to the servers located at the GMC-Site R. Table 5 identifies the specific hardware for use at the GMC locations. The Sparc 20 servers for the GMC-Pentagon and GMC-Site R are on hand while the majority of the remaining hardware is still in the procurement process. Additional changes to the hardware configurations of the GMC locations will occur as GCCS expands and mission needs change.

3.4.6.2 Top Secret Capabilities

The three GMC locations also will require hardware operating at the top secret level to perform system and network management for the top secret component of the GCCS. Again, figures 17, 18, and 19 show the GMC-Pentagon, GMC-Site R, and the GMC-OSF locations getting workstations and servers to perform this function. Specific GMC top secret hardware and software requirements will be determined when the GCCS(T) is architected. The capabilities show in the diagrams are for notional purposes only.

Unless otherwise identified, all hardware purchased is Sun Sparc Workstations of various sizes and capabilities.	Server #1 (Performance Mgmt)	Server #2 (Remedy & Oracle)	Server #3 (Accugraph)	Network Mgmt (Type A)	Network Mgmt (Type B)	Network Mgmt (Type C)	Smart Agent Mgmt	Performance Mgmt	Configuration Mgmt	HelpDesk (Type A)	HelpDesk (Type B)
Hardware											
Sparc 5/85 Hz (base RAM of 32 MB)				1	1	1	1	1	1	1	1
Sparc 20/75 Hz (base RAM of 32 MB)	1	1	1								
Solaris 2.4 Operating System	1	1	1	1	1	1	1	1	1	1	1
32 MB RAM Module	7	7		4	4	4	4	4	4	4	4
64 MB RAM Module			8								
2.1 GB Hard Drive						1	1	1		1	1
4.2 GB Hard Drive (2 x 2.1 GB Drives)				1	1				1		
12.6 GB Hard Drive (6 x 2.1 GB Drives in Array)	1	1	1								
4mm Tape Drive	1	1	1	1	1	1	1	1	1	1	1
CD-ROM	1	1	1	1	1	1	1	1	1	1	1
3.5" Floppy Drive	1	1	1	1	1	1	1	1	1	1	1
PCMCIA Reader	1	1	1	1	1	1	1	1	1	1	1
FDDI Interface Card	1	1	1	1	1	1	1	1	1	1	1
AUI Adapter Cable	1	1	1	1	1	1	1	1	1	1	1
17" Monitor				1	1	1			1	1	
20" Monitor	1	1	1				1	1			1
Printer, Black and White Laser (2 required)											
Printer, Color Laser (2 required)											
Initial Number of GMC Devices at GMC-Pentagon	1	1	1	2	1	1	2	2	2	4	3
Initial Number of GMC Devices at GMC-Site R	1	1	1	1	1	1	1	1	1	2	2
Initial Number of GMC Devices at GMC-OSF				1							1
Initial Number of GMC Devices in Unclassified Developmental Lab at OSF	1	1	1								
Total GMC Server and Terminal Type Hardware Configurations per Type	3	3	3	4	2	2	3	3	3	6	6

Table 5 GMC Hardware Distribution

3.4.6.3 Emergency Dial-in Management Access

One of the major dilemmas facing any manager responsible for system and network management of a diverse system is how to troubleshoot a site when that site has lost network connectivity. The main capability of the GCCS resides around the 37 IOC GCCS sites, specifically the 16 JOPES database sites. The GCCS program deployed Cisco 2511 Communication Servers at the GCCS sites to support dedicated and dial-in circuits to remote users. The management dilemma can be solved by using the dial-in capabilities installed at the 37 IOC GCCS sites to reach through and gain access via this "management backdoor" capability. In essence, the GMC becomes the same as one of the site's remote users except the GMC accesses the management functions and not the site's mission

functionality. All access, authentication, and audit requirements will apply to GMC access just the same as a site's remote user access. Figure 20 shows STU-IIIs used at the GMC locations for this purpose. They will be used to dial into a GCCS site at the secret level. This provides access to a site that is no longer reachable via the WAN. Figures 17, 18, and 19 show the STU-IIIs attached to several of the GMC workstations.

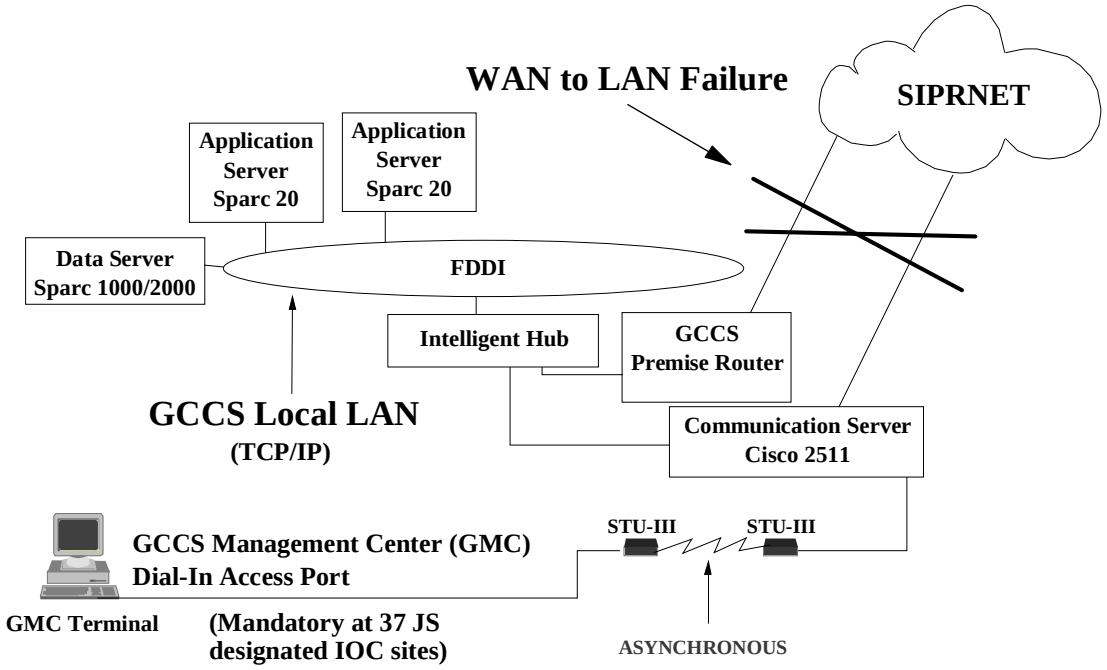


Figure 20 GMC Remote Access via Cisco 2511-CSs

The GCCS sites that received communication servers are listed in Appendix D. Also shown in the appendix are which sites must reserve a port on a communication server for management purposes. The GCCS site will be responsible for requesting a dial-in line for that GMC port and for paying the monthly recurring costs of the telephone circuit. This GMC port must have a dedicated telephone number reserved for use only by the GMC. It will not be used by operational users. DISA/JIEO will provide the STU-III for the GMC port to the GCCS sites. In some cases, when appropriate, the GMC will share access of this dial-in port with S/A management centers responsible for maintaining the GCCS site. For example, the USMC plans to have a single management center controlling the USMC GCCS sites. The telephone numbers for the GMC ports could be shared with the USMC management center so they could also have troubleshooting access to a USMC GCCS site that has lost WAN connectivity.

Intelligent agents, also referred to as smart agents, must be installed at each GCCS site during the fielding process. These smart agents function as the relay point for the events and traps reported by the various management agents installed at that particular location. Before the smart agents forward information to the GMC, they store copies of that information into various log files. In the event of lost WAN connectivity, the emergency dial-in access capability provides the mechanism for reviewing the events in these logs. The smart agents at the sites continue to record site events even after the WAN communications failure. The dial-in backdoor capability to the site's smart agents logs will greatly increase the maintainability of the GCCS.

No dial-in "management backdoor" capabilities are planned for the TS3 at this time under its current architecture. When TS3 migrates to the GCCS (T) the requirements for "backdoor" management access will be reevaluated.

3.4.7 GMC Software Architecture

The GMC will operate using COTS system and network management software. However, there are some GOTS management tools which are used to maintain the JOPES applications and database in the WWMCCS environment. Some of these tools are being migrated from the WWMCCS to the GCCS environment. GOTS will be used only if no COTS products perform that specific management function. Non-COTS proprietary system and network management software will not be used outside of the GOTS tools identified for JOPES.

The GCCS JOPES tools will continue to be used in the GCCS environment to maintain the GCCS JOPES functionality until such time that they can be replaced by COTS applications operating at the GMC and the GCCS sites. This will require future software upgrades to the JOPES mission applications to make them compliant with the Application Program Interfaces (APIs) used by the COTS management software identified for use on the GCCS. Once the JOPES mission applications are API compliant and management functionality has been demonstrated using the COTS programs, the GOTS applications will be deactivated.

The preferred method for managing the GCCS will be "management by exception." This means the reporting of state changes, traps, or critical events will occur without management polling across the network. Polling of device or application status using SNMP can create a tremendous amount of overhead on a network. This in effect reduces the amount of bandwidth available for mission critical data traffic. The main criteria for selecting COTS management applications was the ability of the application to obtain the device or application status without constant polling over the WAN. The design goal of the GMC is that all polling occurs on the local site LAN. If polling is required on the GCCS it will be the responsibility of the Performance Management office to do that polling and then share the polling results real-time with other offices that may need the information. Normal operation though will be for a smart agent to discover an event, trap, or alarm, and then the local agent is to forward the event, trap, or alarm over the WAN to the designated management facilities. For GCCS this is the GMC-Pentagon, the GMC-Site R, and the GMC-OSF. Every effort will be

made to minimize SNMP traffic on site LANs. At the time of this revised publication, no site had more than 0.1 percent of their LAN traffic being SNMP packets.

The software used for system and network management of the GCCS falls into two categories. The first is the COTS management software installed at the GMC locations. Some of these applications will be used only by GMC personnel while others can also be accessed by GCCS site personnel. For example, the Remedy trouble ticketing system will be made available to site personnel. The second category of software is the smart agents that must be installed at each site running the GCCS mission software. The smart agents are the only GMC software being purchased and fielded by DISA to the individual GCCS sites. What COTS management applications are run at GCCS sites is the responsibility of the S/A GCCS PMOs. The smart agents are used to monitor the health and status of the GCCS across the globe. By using the smart agent technology the GMC can fulfill the joint oversight mission without adversely effecting GCCS performance. The following sections will provide additional detail concerning the COTS management software used on the GCCS.

3.4.7.1 Compliance with Standards

All COTS system and network management software used by the GMC must comply fully with ISO standards. Most products currently on the market are based on Simple Network Management Protocol, Version 1 (SNMPv1). SNMP, Version 2 (SNMPv2), was defined as an update to the SNMPv1 management protocol with enhanced security and audit features. However, the Internet committee defining SNMPv2 was in hiatus for the fall of 1995 because the SNMPv2 committee could not decide on which security mechanisms should be included. A new committee has now formed and continues to define SNMPv2. Two sets of Internet Drafts are now being produced to describe the two different security methods being discussed for SNMPv2. Very few product vendors have updated their applications to use SNMPv2 like features at this time. A more recent protocol defined by the ISO organization is the Common Management Information Protocol (CMIP). Again, like SNMPv2, very few vendors have changed their applications to be compliant with this protocol. Realizing that existing system and network management software falls short in many areas, the Network Management Forum organized the OMNIPoint committee. Its purpose is to study existing standards and establish the steps necessary to create more robust management software. The main thrust is on interoperability between products for fault and configuration management.

The GCCS will start by using SNMPv1 compliant management applications. The vendor products used in the GMC will mature and migrate to the newer management protocols in time. Once a product has been upgraded an engineering decision will be made to determine the feasibility and timetable for upgrading that particular application at the GMC. This upgrade will be coordinated with the GCCS DIR to ensure there is no mission impact on GMC capabilities.

Besides being compliant with the ISO standards, all software used for system and network management must be compliant with the DII Runtime Specification for the DII COE. This requires all software to be segmented and integrated into the DII COE. The hardware platforms used for system and network management will adhere to these principles. During the initial building of the

GMC infrastructure this requirement will not be achievable because of time and manpower constraints with meeting the proposed GCCS IOC date. The initial GMC capabilities have been running on the Solaris 2.4 operating system for over a year. Target compliancy with the DII COE is scheduled for Solaris 2.5 which will be in the DII COE Version 3.0. FOC will not be declared for the GMC until all system and network management software at the GMC locations is segmented and running on the DII COE.

3.4.7.2 Initial GMC COTS Products

The following subparagraphs briefly describe the COTS system and network management applications that will be used on the GCCS at the GMC locations (i.e. the Primary LCCs). These tools will not be provided to the GCCS sites (i.e. the Secondary LCCs). It is important to understand that it will take time to configure and build each of these applications. Those responsible for implementing system and network management are concentrating on those applications which will provide fault and performance management at a high level for the start of the user assessment period referred to as Operational Test, Phase 2 (OT-2). This high level look will provide a quick glance at the GCCS during the assessment period to determine if the network bandwidth and architecture will meet the needs of a fully operational GCCS. This quick look will provide a window of opportunity in the event network parameters must be changed or upgraded prior to WWMCCS termination. All of the products listed below for use at the GMC run using the Solaris 2.4 operating system.

3.4.7.2.1 SunConnect, SunNet Manager

SunNet Manager is an SNMP based management platform that relies on the manager-agent model described in the OSI management framework. It also relies on the native Solaris TCP/IP communications for data transport. The manager is a user initiated process and management console with a Graphical User Interface (GUI). The agent is a process that accesses the managed object and collects data on behalf of the manager. Graphics are displayed on an Open Look GUI running under OpenWindows. OpenWindows supports the X.11 display protocol. The SunNet Manager uses predefined icons, also called glyphs, to represent managed network objects. An editing menu provides graphical editing for creating, deleting, cutting, copying, and pasting of glyphs used on the system. Events can be configured with predefined event request properties that are used to specify attributes. A specified attribute can show a visible state change on a glyph. For example, a glyph representing a Sun Sparc 2000 could be made to change colors from green to red if the device no longer can be reached on the network. The SNMP trap daemon is installed with SunNet Manager agents and daemons. The trap daemon translates received SNMP traps and forwards those traps to the Event Dispatcher on one or more management stations. The SNMP trap daemon uses an SNMP trap file to translate trap type numbers to ASCII strings and to determine if the trap should be kept or discarded. The SNMP host file allows mapping of specific devices to traps.

3.4.7.2.2 Solstice Cooperative Console

Solstice Cooperative Consoles (Solstice CC) software interconnects multiple SunConnect SunNet Manager consoles together to enable cooperative management of medium to large enterprise networks. Topology changes as well as event and trap information are forwarded between consoles. Changes to one user's map are automatically reflected on other' maps real-time. Both users can make data requests to components in the common network. Most importantly, Solstice CC allows flexible configurations in how consoles are interconnected and in configuring the amount of management data sent between consoles.

3.4.7.2.3 Hewlett Packard Company, NetMetrix

HP NetMetrix is a distributed network management system that provides troubleshooting, operational, and planning tools to manage Ethernet, Token Ring, and FDDI networks, at the network, segment, conversational, or nodal level. The suite of graphically based tools is used for interpreting events, alarms, and traps collected from the remotely configured remote monitoring (RMON) agents distributed across the GCCS. The product is comprised of a load monitor, a protocol analyzer, an internetwork monitor, a traffic generator, and enterprise utilities. The two specific products used are the NetMetrix Workgroup Analysis Bundle and the NetMetrix Distributed Internetwork Monitoring and Analysis System.

The load monitor is an application that allows the examination of a segment's network load. Network load can be categorized by source, destination, between pairs of nodes, protocol type, over time, or packet size. Categorizing network traffic helps to recognize potential problem areas and can be used to identify elusive performance bottlenecks. Other features include how load and performance vary over time, systems interaction analysis, additional node impact, threshold baseline, network application load generation, and graphical display of RMON traffic. A zoom feature provides the ability to correlate network monitoring statistics into meaningful information. Zoom allows a GMC technician to see who talks to whom, when, and with what protocols, at different OSI layers. The GMC technicians can recreate problem events on the network in real time or in historical mode using the load monitor.

The protocol analyzer looks inside network packets to allow an in-depth analysis of datagrams on the network. It captures individual packets based on easy-to-specify filtering criteria. Packets are displayed based on summary information, detail, and hexadecimal format. Seven-layer decode suites are available for over 100 protocols. The complete feature set includes triggering, pretriggering, slicing, flexible capture buffers, dump to disk, and extensive filtering capability. The protocol analyzer provides the capability for debugging protocols and distributed applications.

The internetwork monitor gathers and correlates data such as network load on multiple segments on an internetwork and integrates that data into a single, comprehensive and logical view. The GMC technician can focus on intersegment traffic, view end-to-end traffic, or see the effects of bridges and routers on their network's traffic pattern. The internetwork monitor allows users to view segment

Media Access Control (MAC) and network levels of an internetwork. Protocol filters are provided so that GMC technicians can see how any protocol affects the internetwork. The internetwork monitor works with the RMON power agent, LanProbe, extended RMON modules, and the load monitor archive file.

The traffic generator lets GMC technicians generate a precise traffic profile to simulate load on the network and test network devices. Utilities provide users with reporting, alarm management, trending tools, and token ring-specific management applications. The traffic generator works simultaneously with all other HP NetMetrix applications so that GMC technicians can see test results in real time.

NetMetrix collected data can be represented in graphical format either in a real time or historical time frame. The graphics can be configured to show bar, plot, pie, or segment graphs. The bar and pie graphs can be shown three dimensionally.

3.4.7.2.4 Legent Corporation, Agent Works Systems Manager

The Legent Agent Works Systems Manager is the managing application complement to the Legent Agent Works UNIX Systems Manager Agent. The two products provide a standardized management and agent software application used to monitor the availability and performance of multi-vendor, distributed UNIX system resources across a network. Systems Manager represents an SNMP based view of multi-vendor UNIX environments. The application provides access to key system attributes such as resources, application activity, and system health. Through the agents, collected workload statistics such as CPU utilization, swap activity, internal memory usage, and hard disk space utilization are sent to the Systems Manager for analysis. The Systems Manager can also provide constant monitoring of key ASCII logfiles to facilitate early detection of faults in the operating system, communications subsystems, and applications running on the target host. It can also monitor key UNIX processes, system security, system fault tracking, and MIB2 connectivity. Alarms can be caught by the GMC and displayed on color coded CAD drawings.

Please note the Legent Corporation was bought out by the Computer Associates (CA) company but CA is continuing the carry the Legent product line at this time.

3.4.7.2.5 Legent Corporation, Agent Works Database Manager for Oracle

The Legent Agent Works Database Manager is a manager and agent software application that is used to monitor Oracle RDBMS availability and performance. The DB manager presents a management view of Oracle RDBMS resources that conform to SNMP using an Open Software Foundation (OSF)/Motif standards based GUI. It is designed to extend the functionality of management platforms by providing the GMC technician a view into critical components of database resources through interaction with the Legent Oracle DB Agent. The main purpose of the DB Manager is to ensure application availability and performance management for the Oracle RDBMS. The DB Manager is capable of auto-discovery, monitoring, providing analysis, and displaying critical Oracle

parameters. Some of the key benefits provided by the DB Manager include its ability to operate in highly distributed environments, provide detailed event, configuration, and status management of the Oracle RDBMS, and its operability with standards-based system and network management applications using SNMP as the management protocol. Several problems have occurred with this smart agent. Most problems encountered are due to the fact that all Sparc 1000/2000 data servers are configured differently instead of being standardized. Further evaluation will be required to see if this smart agent and application can be made to work. Other products will be looked at during this evaluation period to determine the best possible course of action.

3.4.7.2.6 Remedy Corporation, Action Request System Help Desk

The Remedy Action Request System (ARS) manages the timely resolution of support requests or system and network problems. It creates a flexible workflow process for the GMC support staff while automatically capturing a database of problem solving experience. The Remedy ARS is implemented with a client-server architecture giving end users and GMC support staff interactive access to the ARS database. For Help Desk and trouble-ticketing functions, the ARS will provide a wide range of capabilities from issuing trouble tickets, to paging technicians, or maintaining an SQL searchable object oriented history. The ARS can interface with RDBMS platforms or with a flat file structure. The ARS for the GMC will interface with an Oracle RDBMS. Trouble tickets can be submitted automatically by other management applications such as SunNet Manager using the provided APIs. Management applications within GCCS will be configured to take advantage of this autogeneration feature. The query function of the ARS will assist GMC support staff and GCCS site administrators in solving problems by providing a versatile tap into an ever growing knowledge and experience database. The database provides a running history of how previous problems were resolved and can provide insight into future problems. The macro function can be configured to automate frequently performed operations such as a daily report of open, high priority trouble tickets. Specific Remedy products being used at the GMC locations are: the Remedy ARS Server with three fixed write licenses, the Remedy ARS Distributed Server Option, the Remedy ARS Servers to Multi-Processor Option, the Remedy ARS Full-Text Search Floating Licenses (issued in 10-packs), the Remedy ARS Fixed Write Licenses (issued in 5-packs), and the Remedy ARS Floating Write Licenses (issued in 5-packs).

3.4.7.2.7 Accugraph Corporation, Accugraph Physical Network Management Bundle

The Accugraph Physical Network Manager will be used for configuration and asset management. This is based on the product ability to provide the widest range of function, versatility, and ease of integration. Configuration management is provided by associating a managed object with a physical location provided by a CAD drawing. Asset management is a physical inventory list associated with the managed object. A managed object can be any workstation, server, or network device that can be controlled or managed by a logical system or network management application. The Physical Network Manager uses ISO published APIs to directly integrate with other management products such as the Remedy Action Request System previously identified. The advantage of the Accugraph product is that the CAD-like drawings can be linked to the SNMP manager. As a device changes

status with the SNMP manager, this status can be shown on the CAD drawing by changing the color of the icon. Eventually, all GCCS sites will be displayed in Accugraph. Specific Accugraph products used are the Physical Network Management Bundle which has read/write capabilities and the "View Only" Licenses.

3.4.7.2.8 Bay Networks, Optivity LAN for SunNet Manager

Bay Networks is a new company formed by the merger of Wellfleet Communications and the Synoptics Corporation. Optivity provides management capabilities and tools for Synoptics full line of concentrators and intelligent hubs. The Optivity application will be used to provide fault management and configuration management of the intelligent hubs installed at the GCCS sites. The Optivity application enables GMC technicians to isolate and view logical associations of the physical connections among users and devices on a network. Optivity also includes sophisticated rule-based software that alerts the GMC technicians when the network's physical limitations are exceeded.

3.4.7.2.9 Cisco CicsoWorks

The CiscoWorks application from Cisco will be used to view and/or manage the GCCS premise routers. This application can also be used to view backside routers and campus routers. CiscoWorks was chosen because all of the initial GCCS premise routers fielded where manufactured by Cisco.

3.4.7.2.10 Concord Communications, Trakker Network Health

Trakker Network Health provides proactive reporting and graphing capabilities. Daily reports can be generated to indicate the current state of the network. Trend analysis can give advance notice of upcoming or potential problems. Trakker is capable of retrieving vital statistics from hub MIBs, RMONs, or other smart agents. This information then can be stored into a relational database for later manipulation.

3.4.7.2.11 Initial COTS Software Distribution

Table 6 identifies how the GMC software will be loaded at the three GMC locations. When possible, software licenses purchased were for concurrent user operations and not fixed user operations. This reduces the number of required licenses and also provides a mechanism by which GCCS site personnel can be given access to the GMC functionality. By using the table below, Table 6, and Figures 17, 18, and 19, the initial GMC architecture is defined for managing the GCCS.

Unless otherwise identified, all software purchased is for the Solaris 2.4 Operating System with the exception of the Smart Agents that are deployed to the GCCS sites. The Smart Agents are GCCS COE compliant on Solaris 2.3.	Required at GMC Locations	Required at GCCS Sites	Server #1 (Performance Mgmt)	Server #2 (Remedy & Oracle)	Server #3 (Accugraph)	Network Mgmt (Type A)	Network Mgmt (Type B)	Network Mgmt (Type C)	Smart Agent Mgmt	Performance Mgmt	Configuration Mgmt	HelpDesk (Type A)	HelpDesk (Type B)
Software													
Accugraph "View Only" License	Y					1	1	1	1	1		1	1
Accugraph "Write/View" License	Y										1		
Accugraph Physical Network Management Bundle License	Y				1								
Bay Networks Optivity Internetwork	Y					1							
Bay Networks Optivity LAN for SunNet Manager	Y					1							
CA/Legent AgentWorks Database Management Agent	Y	Y											
CA/Legent AgentWorks Domain Manager	Y						1						
CiscoWorks	Y					1							
Concord Trakker Network Health	Y		1				1						
Concord Universal Poller	Y		1				1						
Cooperative Console License	Y		1			1		1	1	1	1	1	
Empire UNIX Systems Management Agent	Y	Y											
HP NetMetrix Distributed Internetwork Monitoring Analysis System	Y		1										
HP NetMetrix Remote Monitoring Agent	Y	Y											
HP NetMetrix Workgroup Anaysis Bundle	Y		1										
Oracle Parallel Query Option Concurrent for 40 users	Y			1									
Oracle RDBMS 7.1.4 Concurrent for 40 users	Y			1									
Oracle SQL *NET & TCP/IP Concurrent for 40 users	Y			1									
Oracle SQL *Plus	Y			1									
Remedy ARS Distributed Server Option	Y			1									
Remedy ARS Flashboards	Y			1						1			
Remedy ARS Full-Text Search Floating License (10-pack)	Y			1		1	1	1	1	1	1	1	1
Remedy ARS Server (w/3 fixed write licenses)	Y			1									
Remedy ARS Servers to Multi-Process Option	Y			1									
Developer 2000 (MS Windows) (Pentagon & OSF Unclass Dev LAB)	Y												
Developer 2000 (Solaris OS) (OSF Unclass Dev LAB)	Y												
Remedy Fixed Write License 5-pack (Solaris OS/standard database)	Y												
Remedy Floating Write License 5-pack (MS Windows/standard database)	Y												
Remedy Floating Write License 5-pack (Solaris OS/standard database)	Y			1		1	1	1	1	1	1	1	1
SunNet Manager License	Y		1			1		1	1	1	1	1	
Initial Number of GMC Devices at GMC-Pentagon			1	1	1	2	1	1	2	2	2	4	3
Initial Number of GMC Devices at GMC-Site R			1	1	1	1	1	1	1	1	1	2	2
Initial Number of GMC Devices at GMC-OSF						1							1
Initial Number of GMC Devices in Unclassified Developmental Lab at OSF			1	1	1								
Total GMC Server and Terminal Type Software Configurations per Type			3	3	3	4	2	2	3	3	3	6	6

Table 6 GMC Software Distribution

3.4.7.3 Initial GOTS Products

DISA/JIEO was tasked by the Joint Staff to ensure the functionality of the tools currently used by the WWMCCS JOPES FDBMs and TDBMs would exist in the GCCS environment. The JOPES

applications migrated to the GCCS environment do not contain any APIs that can be used by the COTS system and network management software used at the GMC. As such, the tools used in WWMCCS had to be migrated to the GCCS environment. Scientific Research Association (SRA), under contract with DISA, was tasked to migrate these tools to the GCCS. The tools used to support JOPES management functionality are called "GCCS System Services" and will be explained in greater detail in the following section. The goal of future releases of GCCS JOPES applications will be to eliminate GOTS management tools by incorporating APIs into the applications that can be accessed by the COTS management applications. The GCCS System Services application will be loaded on an as-needed basis for each of the GMC client workstations.

3.4.7.3.1 GCCS System Services

The GCCS System Services developed by SRA is used to manage portions of the JOPES functionality within GCCS. The GCCS System Services main menu contains seven major areas. These major areas will be discussed briefly in the following paragraphs. The seven areas are:

- System Services Utilities
- Journaling
- Monitors
- Audit Reports
- Plan Management
- Merge TPFDD
- Create TPFDD file

The System Service Utilities menu will be used for transaction processing management, transaction distribution management, Transaction Distribution System (TDS) network management, and configuring the external transaction processor. Some of the functions will be activating or terminating the processor, enabling incoming and outgoing transactions, and setting up the TDS locations. The external transaction processor will set up file names and identify how the process operates, foreground or background.

The Journaling menu will be used to set tape parameters for journaling purposes. Some of the functions are setting the auto journal time interval, terminating an auto journal, archiving journal sets to tape, or resetting the journaling subsystem. This menu also provides a place to set printing options for the journal status, log, and list outputs.

The Monitors menu will be used to look at various activities occurring with the JOPES functionality. This includes looking at the receive queue detail, the receive queue summary, the send queue detail and the TDS monitor. Each of these monitor details will be used to show the health of transactions flowing between the JOPES section of the GCCS Sparc 1000 or Sparc 2000 database servers.

The Audit Reports menu will be used to monitor the database servers accessibility, perform load selection, configure report selections, set User IDs, set transaction parameters, and select carrier requirements. These menus will allow for the orderly flow of transactions within the JOPES applications.

The Plan Management menu is used in conjunction with the OPLANs used by the GCCS JOPES applications. Some of the functions are plan maintenance, setting user permissions, and generating a user permissions report. Also included is the ability to off-load or reload a plan, perform local recovery of an OPLAN, and recover site data. The next menu shows the status of an OPLAN as it exists across the GCCS servers. The final menu allows for a TPFDD to be loaded into an OPLAN.

The Merge TPFDD is used to join TPFDDs files for inclusion in OPLANs. Some of the functions include setting the target OPLAN, selecting source files and tapes, limiting the records to be merged, limiting who can access the new file, and initiating the merge.

The Create TPFDD File menus will be used to create new TPFDDs. Some of the functions include setting the file names and locations, determining what accesses and permissions apply, and setting the record parameters.

3.4.7.3.2 Other GOTS Products

No other GOTS system and/or network management tools exist within the GCCS Version 2.0, Version 2.1, or Version 2.2 releases. Every effort will be made by DISA to ensure future GCCS applications do not require additional GOTS management tools, but instead can be managed by the COTS applications running at the GMC.

3.4.7.4 Management Information Base (MIB) Requirements

Three Management Information Bases (MIBs) will be used to mange the GCCS servers and LANs. They are the Database (DB) MIB, the Host Resources (HR) MIB, and the Remote Monitoring (RMON) MIB. The MIBs will be used for monitoring the Oracle database, UNIX system operations and performance, and network segment operations respectively.

The DB MIB defines the facilities for managing relational database implementations. Information such as database product, database table, servers, and connections enables the GMC to track databases of various GCCS applications. Control of this function could be passed to other support facilities within the GCCS while the GMC will ensure interoperability and consistency among the data sets.

The HR MIB defines the facilities for monitoring UNIX system operation such as main memory size, disk storage information, peripheral devices, and system information such as operating system configuration, process information, CPU utilization, and product application information.

The RMON MIB defines the facilities for monitoring upper layer application entity connection and loading information. The RMON MIB is used to evaluate the network efficiency of the client-server software implementation by monitoring a database or application server. It can be used to minimize the impact of resource limitations by deconflicting network resources. The RMON MIB also can be used to provide capacity planning information as the basis for future changes.

3.4.7.5 GCCS Smart Agent Types and Locations

Four different smart agents were identified for initial use in the GCCS. The four smart agents help the GMC monitor the health of the GCCS by concentrating on the Oracle database health, UNIX system operations and performance, and network segment operations respectively. Other smart agents will be added to the GCCS management architecture as the GCCS matures to include additional hardware platforms and operating systems. Each of the smart agents are briefly discussed below. Also Figure 21 shows where the smart agents must be installed at a GCCS site.

The Hewlett-Packard Remote Monitoring (RMON) Agent monitors utilization rates and errors of the GCCS LANs. One copy of the RMON agent is required per LAN segment. Do not install multiple RMON agents on the same LAN segment because this is redundant and unnecessary. The smart agent allows profiling the top 10 users, the top 10 conversations, a breakdown by protocol of the number of packets sent on the LAN, and any duplicate IP addresses that reside on that LAN. The statistics are gathered for a 24 hour period and then sent via SMTP to the GMC. The RMON agent also generates traps when certain thresholds are exceeded throughout the 24 hour period and these are sent immediately to the GMC.

The Empire UNIX System Manager Agent monitors the operation and performance of the UNIX platforms. The agent must be installed on each of the Sparc data, application, and EM servers. The smart agent monitors free space for all available disk partitions and also monitors CPU load indicators. The smart agent generates traps when thresholds are exceeded and immediately sends an SNMP message to the GMC. Exploration is underway now to find an equivalent smart agent for use with the HP operating systems used for the TAC-3s and TAC-4s. Thus if a TAC is configured to run as an application or EM server the health of that platform can be monitored.

The Legent UNIX System Manager Agent also monitors the operation and performance of the UNIX platforms. The agent was to have been installed on the Sparc EM servers. However, online performance comparisons showed the Empire UNIX System Manager Agent performed the role better than the Legent UNIX System Manager Agent. Therefore the Legent UNIX System Manager Agent will not be installed on the GCCS.

The Legent Oracle DB Agent monitors the status of the Oracle RDBMS running on the database server. The agent monitors table space utilization, hotdisk and hotfile statistics and the fragmentation percentage of tables and table spaces. The smart agent was to have been installed on each database server supporting the JOPES Oracle database. As previously stated, several problems have occurred with this smart agent. Most problems encountered are due to the fact that no two Sparc 1000/2000 data servers are configured the same. Further evaluation will be required to see if this smart agent and application can be made to work in the GCCS environment. It may require that the smart agent be customized at each location because of the differences in configurations. During the evaluation period other products will be looked at to determine the best possible course of action. Consult the GCCS classified web site for further information as it becomes available.

Figure 21 shows where the smart agents must be installed at a GCCS sites. The HP RMON smart agent is to be installed on each LAN segment. The Empire UNIX System Manager smart agent must be installed on all data, application, and EM servers. During the loading of the smart agents they must be configured to report to the GMC-Pentagon and the GMC-Site R. Also at this time if the site has an SNMP management station in operation the IP address or DNS name of this device can be added to the smart agents' configuration files. This way the site can receive the fault and performance information and statistics at the same time the GMC locations do.

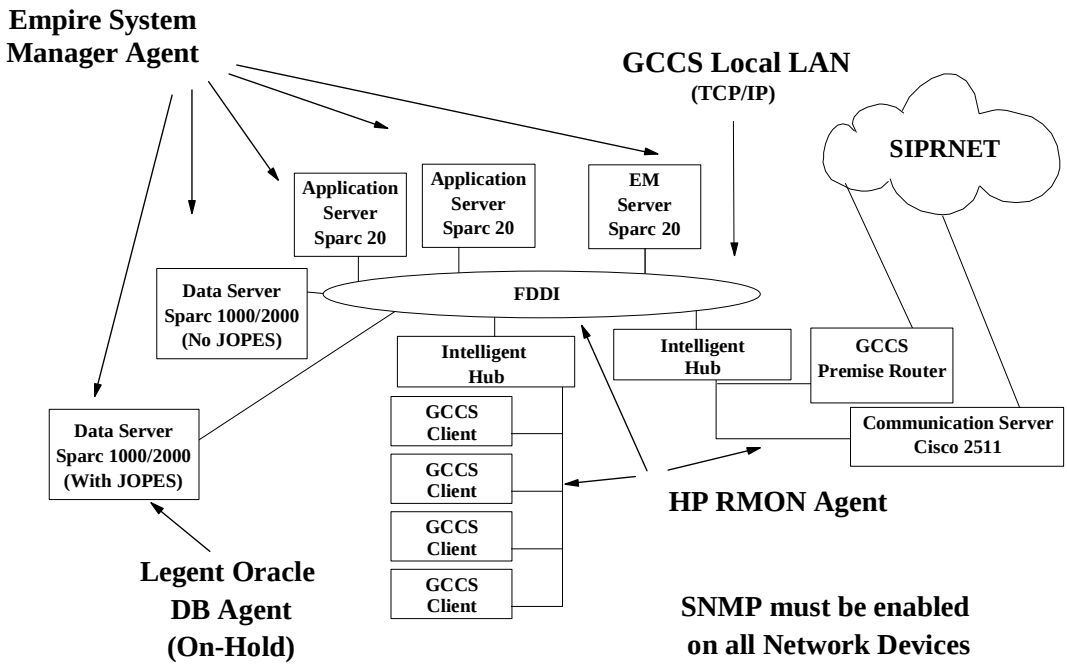


Figure 21 Smart Agent Locations at GCCS Sites

3.4.7.6 Future GMC Software Upgrade Procedures

As the GCCS matures the system and network management software used at the GMC will change. This may be because a COTS software package has a new release, the DII changes what software it uses, a better COTS product is identified to replace existing functionality, or the Joint Staff rolls in a new requirement that changes how business is being done. Any of these changes will require upgrades at the GMC locations and possibly to the smart agents deployed at the GCCS sites.

The GCCS DIR, in conjunction with the GCCS Engineering Office, will make the determination to add, replace, or delete any system or network management software. Once a change has been approved the candidate software will undergo testing at the OSF in an unclassified, off-line mode. Only after the software has passed all quality control checks and product assurance testing will it be transitioned into the operational GMC infrastructure.

3.4.8 Manpower Personnel Definitions

The following subsections will describe the various positions and duties required at different levels with the GCCS structure. The terms defined in this section will be used throughout the remainder of the document when describing personnel responsibilities. This section is intended to provide a partial mapping from WWMCCS personnel and required functions to those personnel and functions required in the GCCS. It is not intended to be an all encompassing job description for the GCCS positions. Required revisions to many of the existing WWMCCS related Joint Pubs will define the GCCS personnel job descriptions concisely. The positions will be filled by military or civilian equivalent individuals.

3.4.8.1 Joint Staff Positions

The following subsections will describe the various positions and duties required at the Joint Staff level to support the GCCS.

3.4.8.1.1 Data Information Coordination Office (DICO)

The Director for Operations (J-3), Joint Staff, will designate a Data Information Coordination Office (DICO) to provide operational direction and guidance for the GCCS. This position was also designated the DICO in the WWMCCS environment.

3.4.8.1.2 GCCS Director (GCCS DIR)

The Director for Command, Control, Communications, and Computers (J-6), Joint Staff, will designate a GCCS Director (GCCS DIR). The GCCS DIR will be the focal point for all aspects of GCCS operations related to system and network configuration, fault, performance, and security management. This responsibility includes testing, evaluation, and implementation of the GCCS. This position was known as the WIN Director in the WWMCCS environment. The GCCS DIR will provide technical solutions to the DICO for an operational decision on global GCCS problems or recommended changes.

3.4.8.1.3 GCCS Designated Approving Authority (DAA)

The Director for Command, Control, Communications, and Computer Systems, (J-6), is the Designated Approving Authority (DAA) for all GCCS security matters. The DAA is responsible for approving security policies, providing security guidance, and taking whatever actions are necessary

to ensure the integrity and security of the GCCS operations. These duties are similar to those currently identified in Joint Pub 6-03.7 for the WWMCCS environment but expanded to incorporate the newer technologies used in the GCCS. Responsibilities and duties for the DAA for GCCS are outlined in CJCSI 6731.01.

3.4.8.1.4 GCCS Security Officer (GSO)

The Director for Command, Control, Communications, and Computers (J-6), Joint Staff, will designate a GCCS Security Officer (GSO). The GSO is responsible for the day to day security operations of the GCCS. As such, all Site GCCS Information System Security Officers (Site GCCS ISSOs) will be responsible to the GSO. The GSO is responsible for providing security information and recommendations to the Joint Staff DAA for matters involving the GCCS. Responsibilities and duties for the GSO are outlined in CJCSI 6731.01.

3.4.8.2 GMC Positions

The following subsections will describe the various positions and duties required to support the GCCS at the GMC level. Described will be the positions required for the GMC-Pentagon, GMC-Site R, and GMC-OSF.

3.4.8.2.1 Chief, GMC-Pentagon

This position will be in charge of all GMC technicians assigned to the GMC-Pentagon and will be responsible for the day-to-day operations and management of the GCCS. The individual will receive guidance and direction from the GCCS DIR. The individual will be responsible for ensuring the GMC-Pentagon has adequate resources in terms of manpower, hardware, software, and training to perform its mission.

3.4.8.2.2 Chief, GMC-Site R

This individual will be in charge of all GMC technicians assigned to the GMC-Site R and will be responsible for assuming the day-to-day operations and management of the GCCS in the event the GMC-Pentagon is unable. The individual will receive guidance and direction from the Chief, GMC-Pentagon. In the event the Chief of the GMC-Pentagon is rendered unreachable the Chief, GMC-Site R, will interact directly with the GCCS DIR. The individual will be responsible for ensuring the GMC-Site R has adequate resources in terms of manpower, hardware, software, and training to perform its mission.

3.4.8.2.3 Chief, GMC-OSF

This individual will be in charge of all GMC technicians assigned to the GMC-OSF. The individual will be responsible for the planning and engineering management of the GCCS. The individual will receive guidance and direction from the Chief, GMC-Pentagon, and the GCCS Engineering Office.

The individual will be responsible for ensuring the GMC-OSF has adequate resources in terms of manpower, hardware, software, and training to perform its mission.

3.4.8.2.4 Chief, GMC-JOPES Support Center

This individual will be in charge of all GMC technicians assigned to the GMC-JOPES office and will be responsible for assuming the day-to-day support operations and system management of the JOPES applications within the GCCS. The individual will receive guidance and direction from the Chief, GMC-Pentagon. In the event the Chief, GMC-Site R, is in operational control of the GCCS, the Chief, GMC-JOPES, will receive the guidance and direction from the Chief, GMC-Site R. If both the GMC-Pentagon and the GMC-Site R are rendered unreachable, the Chief, GMC-JOPES, will interact directly with the GCCS DIR. The individual will be responsible for ensuring the GMC-JOPES office has adequate resources in terms of manpower, hardware, software, and training to perform its mission. Once the GMC-JOPES functionality has transitioned to the GMC-Pentagon this position no longer will be required.

3.4.8.2.5 GMC-HelpDesk Supervisor

The GMC-HelpDesk Supervisor will be in charge of all GMC technicians assigned to perform the Help Desk function. The supervisor will receive guidance and direction from the Chief, GMC-Pentagon. In the event the GMC-Site R is in operational control of the GCCS the GMC-HelpDesk Supervisor will receive the guidance and direction from the Chief, GMC-Site R. If both the GMC-Pentagon and the GMC-Site R are rendered unreachable the GMC-HelpDesk will interact directly with the GCCS DIR. The supervisor will be responsible for ensuring the GMC-HelpDesk office is adequately supported by the main GMC to which they are attached. The GMC-HelpDesk Supervisor should become the resident expert in the Remedy Corporation Action Request System used for trouble tickets and the Accugraph Corporation, Accugraph Physical Network Manager used for configuration management.

3.4.8.2.6 GMC Technicians

The GMC technicians will be responsible for the day-to-day support operations of the GCCS. All technicians must be proficient in the COTS and GOTS system and network management software used to support the GCCS. It is not expected that each technician be an expert in all management applications. Rather, the OICs of the three main locations should ensure a diverse coverage of skills to provide adequate management coverage of the GCCS at all times. The technicians will be responsible to the OIC or supervisor in charge of their location.

3.4.8.3 GCCS Site Positions

The following subsections will describe the various positions and duties required to support the GCCS at the GCCS site level. Paragraph 4.8 will discuss in greater detail the required personnel at each GCCS site.

3.4.8.3.1 GCCS Site Coordinator (GSC)

The GSC is responsible for coordinating all system and network support activities within the GCCS site. The individual filling this role will be the primary focal point for coordinating with the GMC and other GCCS organizations. One of the major duties of this position will be to direct activities during and following an emergency condition to minimize the loss of GCCS mission capabilities at the site. For large organizations, the site commander or DAA may want to appoint additional personnel in this function. They will be referred to as an Assistant GCCS Site Coordinator (AGSC). This position was previously known as the WIN Site Coordinator.

3.4.8.3.2 GCCS Network Administrator (GNA)

The GNA is responsible for the day-to-day operation of the GCCS LAN, the data and applications servers, the communications devices (premise router, communications server, and intelligent hubs) and related GCCS equipment. A few of the duties are:

- Maintain the LAN
- Maintain the AUTODIN/DMS (future) interface
- Identify and be capable of installing each LAN component
- Maintain the LAN system interface
- Operate the LAN
- Troubleshoot network and communications problems
- Provide expertise in TCP/IP services

This position was not recognized formally within the WWMCCS environment though most WWMCCS sites had maintenance personnel performing this function.

3.4.8.3.3 GCCS System Administrator (GSA)

The GSA is responsible for a variety of duties with the major focus being on maintaining the GCCS applications, providing local user support, and troubleshooting site problems associated with the GCCS applications. This includes the responsibility of determining if the GCCS applications are properly storing correctly formatted data to the GCCS database servers. A few of the duties are:

- Direct activities during and following an emergency condition to minimize the loss of GCCS mission capabilities at the site
- Maintain access permission lists
- Maintain the Executive Manager permissions program
- Add and remove hardware and software at the local site
- Perform system startups and backups
- Generate periodic summaries of system performance and utilization
- Routinely backup data and audit files
- Setup GCCS User IDs and initial passwords

- Coordinate database modifications with other site personnel and the GMC-Pentagon
- Diagnose system problems and report them to the GSC and GMC-HelpDesk
- Monitor total system performance to ensure optimal performance
- Reconfigure GCCS to regain processing capabilities for non-routine equipment malfunctions
- Assist users in determining the cause of failures

A thorough understanding of the DII COE and software philosophies will be instrumental in accomplishing the duties of this position. This new position most closely matches the WWMCCS position that was previously held by the informal system administrator at a WWMCCS site.

3.4.8.3.4 GCCS Database Administrator (GDBA)

The GDBA is responsible for the day-to-day operations of the databases located at the GCCS site. This may include the primary database server (Sun Sparc 1000 or Sparc 2000) running the Oracle RDBMS, or the Executive Manager application using the Sybase RDBMS, or the AMHS server application using the Verity Topic RDBMS. If the GCCS site does not have any of these databases this position may be vacant. A few of the duties are:

- Coordinate incremental/partial backups of the databases with the GSC and the GMC-Pentagon
- Generate periodic summaries of database performance and utilization
- Coordinate and maintain database modifications
- Monitor all database applications for proper performance
- Manage disk/tape storage

This position most closely matches the shared responsibilities of the TDBM and the site's system DB personnel.

3.4.8.3.5 Site GCCS Designated Approving Authority (Site GCCS DAA)

The Site GCCS DAA is responsible for local security policies and guidance to ensure the integrity and security of the GCCS operations are maintained. Receives direction and guidance from the Joint Staff GCCS DAA. These duties will be similar to those performed by the Site DAAs who supported WWMCCS. The Site GCCS DAA is responsible for accrediting GCCS at the site.

3.4.8.3.6 Site GCCS Information System Security Officer (Site GCCS ISSO)

The Site GCCS ISSO is responsible for ensuring the integrity and security of the local GCCS system and network. This position was previously known as the WASSO. The Site GCCS ISSO is responsible for providing security information to the Site GCCS DAAs. The duties of the Site GCCS ISSO are identified in CJCSI 6731.01. The GMC will be supported by the Site GCCS ISSO appointed at these locations.

3.4.9 GMC Personnel Requirements

The following subsections will describe the manpower for the GMC. The main purpose is to identify what billets will be used in the GMC infrastructure. Positions will be filled by military or civilian equivalents of the appropriate rank or grade.

3.4.9.1 GMC-Pentagon

The GMC-Pentagon is organized and manned by DISA/WESTHEM/JSSC personnel. Current WWMCCS missions have been expanded, and personnel trained and reallocated to both operate and manage GCCS and WWMCCS, until WWMCCS is turned off, and to perform the management functions for network and system management, the GMC-HelpDesk, JOPES, and GSORTS. Additionally, the GMC-Pentagon must also have sufficient manpower to serve as the Secondary LCC for the DISA sponsored NMCC as discussed in section 3.4.5.2.

3.4.9.2 GMC-Site R

The GMC-Site R is organized and manned by DISA/WESTHEM/JSSC personnel. The facility is manned 24 hours a day, 7 days a week. The GMC-Pentagon functions are mirrored in hardware and software at the GMC-Site R facility. The GMC-Site R is minimally manned with a caretaker staff. The GMC-Site R will be augmented and brought up to full strength with GMC-Pentagon and other DISA personnel during GMC-Pentagon extended outages when the GMC-Site R has assumed operational control of the GCCS.

3.4.9.3 GMC-OSF

The GMC-OSF is manned by DISA Center for Computer System Engineering personnel (DISA/JEX) or their designated contractor support. The JEX personnel will perform the role of maintaining the GMC-OSF hardware and software. The GMC-OSF will operate on a normal business week schedule. The GMC-OSF will be used by the DISA Center for Computer System Engineering and the GCCS Engineering Office for long term planning and engineering purposes.

4.0 GCCS OPERATIONAL MANAGEMENT RESPONSIBILITIES

4.1 Introduction and Assumptions

This section describes the day-to-day operational management responsibilities of the various DoD organizations associated with the GCCS. The primary purpose of the following sections will be to delineate which organizations have primary management responsibility over the various portions of the GCCS. The responsibilities described herein also must accommodate a smooth integration into the longer term DIICC requirements.

The responsibilities described in this section are predicated upon the following assumptions:

- The SIPRNET WAN architecture will be sufficiently large to meet the wartime demands of the DoD secret level user communities.
- The GCCS access lines to the SIPRNET will be sized to meet the CINC's or S/A's data requirements.
- The AFC2N WAN architecture will be sufficiently large to meet the wartime demands of the AF GCCS secret level user community.
- The GCCS access lines to the AFC2N will be sized to meet the AF sites' data requirements.
- The crossover trunks from the AFC2N to the SIPRNET will be sufficiently large to meet the wartime demands of AF GCCS users communicating with the rest of the GCCS user community.
- The Marine Corps uses DISN as it's backbone bandwidth provider.
- The SIPRNET access lines to the SIPRNET backbone from USMC sites will be sized to meet USMC sites data requirements.
- The SCAMPI multiplexer network with SOCOM's embedded WAN architecture will be sufficiently large to meet the wartime demands of SOCOM's GCCS secret level user community.
- The GCCS access lines on the SCAMPI multiplexer network will be sized to meet SOCOM's data requirements.
- The crossover trunks from the SCAMPI embedded WAN architecture to the SIPRNET will be sufficiently large to meet the wartime demands of SOCOM GCCS users communicating with the rest of the GCCS user community.
- DISA continues to own, operate, and manage the DISN SIPRNET WAN.
- The AF continues to own, operate, and manage the AFC2N WAN.
- SOCOM continues to own, operate, and manage the SCAMPI network.
- The DISA unclassified Network Information Center (NIC) or the secret level SIPRNET Support Center provides network registration services for Internet Protocol (IP) network numbers, Domain Name Service (DNS), X.400/500 Directory Service, etc for the DoD community.
- The CINCs and S/As manage and maintain their own service or CINC unique information systems as required.

- The CINCs and S/As manage and maintain their own LAN systems as required.
- The GCCS data services are organized in both matrix and hierarchy formats.
- The Joint Staff's JOPES system management requirements transition to the GMC.
- The JOPES Support Branch (TDBM) requirements transition to the GMC.
- The Joint Staff's WIN NOC network management requirements transition to GMC.
- A balance will be maintained between the geographically hierarchical network management of the DISN/DII and the organizationally peered GMC of the GCCS.

4.2 Joint Staff

The Chairman of the Joint Chiefs of Staff is responsible for policy guidance and oversight of the GCCS. The Director for Operations, Joint Staff (J-3), exercises operational control over the GCCS based on the guidance from the Chairman and approves all policy for the GCCS. The Director for Command, Control, Communications, and Computer Systems, Joint Staff (J-6) provides oversight of the system and network management of the GCCS.

4.2.1 J-3/GCCS Data Information Coordination Officer (DICO)

The Director for Operations (J-3), Joint Staff, will designate a Data Information Coordination Office (DICO) to provide operational direction and guidance for the GCCS. This position was also designated the DICO in the WWMCCS environment.

4.2.2 J-6/GCCS Director (GCCS DIR)

The Director for Command, Control, Communications, and Computer Systems (J-6), Joint Staff, will designate a GCCS Director (GCCS DIR). The GCCS DIR will be the focal point for all aspects of GCCS operations related to system and network configuration, fault, performance, and security management. This responsibility includes testing, evaluation, and implementation of the GCCS applications. The GCCS DIR will perform these responsibilities with assistance from various DISA support activities. This position was known as the WIN Director in the WWMCCS environment. The GCCS DIR will provide technical solutions to the DICO for an operational decision on global GCCS problems or recommended changes.

4.2.3 J-6/GCCS Designated Approving Authority (GCCS DAA) for Security

The Director for Command, Control, Communications, and Computer Systems, (J-6), is the Designated Approving Authority (DAA) for all GCCS security matters. He is responsible for approving security policies, providing security guidance, and taking whatever actions are necessary to ensure the integrity and security of the GCCS operations. These duties are similar to those currently identified in Joint Pub 6-03.7 for the WWMCCS environment but expanded to incorporate the newer technologies used in the GCCS. Responsibilities and duties for the DAA for GCCS are outlined in CJCSI 6731.01.

4.2.4 J-6/GCCS Security Officer (GSO)

The Director for Command, Control, Communications, and Computer Systems (J-6), Joint Staff, will designate a GCCS Security Officer (GSO). The GSO is responsible for the day to day security operations of the GCCS. As such, all Site GCCS ISSOs will be responsible to the Joint Staff GSO. Responsibilities and duties for the GSO are outlined in CJCSI 6731.01.

4.2.5 GCCS Operational Modes

The WWMCCS environment specified five WIN Modes of Operation as defined in *Joint Publication 6-03.14, Operation and Management of the WWMCCS Intercomputer Network (Current Edition)*. In the WWMCCS environment these modes of operation were internal to the WWMCCS community and did not specifically apply to the DSNET2 of which the WWMCCS community had exclusive use. However, the DDN did have a minimize procedure in place for each of the four networks; MILNET, DSNET1, DSNET2, and DSNET3. Another change is the C2 community no longer has exclusive use of a data network. The GCCS community does not enjoy exclusive use of the SIPRNET, AFC2N, or the SCAMPI networks. For example, on the SIPRNET, the common user DoD network, GCCS is only 15 percent of the subscribers using the network. It is difficult for one subscriber community to receive a different level of service when the SIPRNET must operate under Defense Business Operating Fund policies. All subscribers pay the same rates and should receive the same level of service.

The internal Priority-Mode operating concept also applies to the GCCS environment, but will be limited to the GCCS sites like it was in the WWMCCS environment. It does not apply to the SIPRNET or other supporting communications infrastructures (AFC2N and SCAMPI). This should not concern the GCCS community provided the WANs maintain proper performance levels, especially the SIPRNET. DISA/D3 maintains the performance criteria specified for day-to-day operations of the SIPRNET. The SIPRNET is to be operated with an overall bandwidth utilization of no greater than 60 percent for the WAN structure. This 40 percent expansion capability should provide adequate available bandwidth to meet the surge required during wartime and crisis situations. If the DISA/D3 office responsible for providing data services for the DII/DISN can not meet the performance criteria of 40 percent unused bandwidth, then other methods will need to be engineered or implemented to support the C2 community bandwidth requirements. As such this will require the DII/DISN PMO to either engineer a technically feasible prioritization scheme based on protocols or to develop operational administrative minimize procedures for use on the SIPRNET. As a near term solution, the DISN PMO is drafting a minimize policy and procedures for use on the NIPRNET and SIPRNET similar to the minimize procedure used on the DDN (MILNET, DSNET1, DSNET2, and DSNET3). It is imperative that the DISA/D3 offices responsible for the SIPRNET provide the proper data communications for the C2 community.

Unfortunately a large number of smaller GCCS sites gain access through one of the S/A or CINC WANs. The Joint Staff J-3 and J-6 offices will have to coordinate with the program manager offices of the AFC2N, USMC NOC, and SCAMPI to ensure they can meet the command and control

community's needs. The WAN networks will have to be large enough to ensure sufficient bandwidth is available to meet wartime needs. Additionally, there must be minimize policies in place for each of these networks in case bandwidth does become a problem.

During Priority-Mode operations, the DII/DISN GCC/RCCs and the S/A and CINC WAN management centers must work in a collaborative effort with the J3 DICO, through the GMC-Pentagon, to provide the best possible service to the GCCS community. All efforts will be made to not adversely effect the remaining SIPRNET and S/A and CINC WAN user communities.

GCCS operations fall into two categories as designated by the DICO, Routine-Mode and Priority-Mode. Routine-Mode describes day-to-day operations while Priority-Mode describes five levels of exercise or crises situations. During a Priority-Mode of operations, all GCCS site operations will be subordinated to the J3 DICO. The J3 DICO will have the authority to determine and/or limit the types of applications executed at the GCCS sites, priority of repairs, manning requirements, and any other activity deemed critical to the operation of the GCCS. Table 7 defines the 5 levels of Priority-Mode operations.

Only the Director, J-3, Joint Staff, or the CINCs will have the authority to declare a Priority-Mode. When a Priority-Mode is declared, the J3 DICO will inform all sites and assumes a heightened state of operational control of the sites involved. During Priority-Mode operations levels 1 and 2, the DISN GCC and the S/A and CINC WAN management centers will be under the direct authority of the GCCS DIR.

Declaration of a priority mode will normally be announced via a Joint Staff J-3 AUTODIN message stating the priority level and the GCCS sites that are included. The message also may include information on related NewsGroup teleconferences that may be in effect for the priority mode of operation. The GMC-Pentagon will also transmit this message directly to GCCS Site Coordinators via electronic mail (e-mail) across the SIPRNET and via the GCCS.GMC.HELP (formerly WWMCCS WIN NOC Teleconference) NewsGroup teleconference.

Priority Level	Condition	Command Authority

5	Command Special Operation	As directed by the CINC with notification to the GMC Director
4	Command Exercise	As announced by the GMC-Pentagon upon recommendation of the CINC in coordination with the Data Information Coordination Officer
3	JCS Exercise	As directed by the Director, J-3, the Joint Staff
2	Regional or Local Crisis	As announced by the GMC-Pentagon upon recommendation of the regional CINC in coordination with the Director, J-3, the Joint Staff
1	Worldwide Crisis	As directed by the Director, J-3, the Joint Staff

Table 7 GCCS Priority-Mode of Operations Levels

During the priority mode of operations, compliance with GMC-Pentagon instructions for site restoral and troubleshooting actions will be required within 15 minutes. If local operational conditions preclude compliance with the request within this time frame, the local GCCS Site Coordinator should request resolution from the DICO. The Joint Staff DICO must be contacted, and then the GMC-Pentagon informed that a resolution has been requested within the same 15-minute time frame.

4.3 CINCs and Services/Agencies (S/As)

The GCCS assets exist in both fixed and deployed environments. The CINCs and S/As have the responsibility for managing the GCCS assets at their local sites because they are the primary owners of the equipment. The CINCs and S/As are responsible for directing their warfighting capabilities based on decisions made via the GCCS DIR and the J3 DICO. As such, the CINCs and S/As are responsible for having adequate support personnel and programmed monies to keep their GCCS site operational. Personnel are responsible for the software, hardware, and security arenas of the GCCS. Funds are needed for equipment upgrades and replacements, maintenance contracts, WAN access circuit costs, and a multitude of other financial requirements. It is the responsibility of the CINCs and S/As to ensure their sites can perform their C2 mission.

4.4 Joint Task Forces (JTFs)

The JTFs are specialized components of the GCCS operating off of deployed assets. The JTFs have a responsibility to manage their assets as part of their local DII global/regional/local hierarchy. The structural hierarchy for management of the JTF assets is mission-oriented rather than geographically-oriented as in the communications part of the DII. This means that instead of sites being managerially associated in a virtual global/regional/local topology, the managerial association is based upon specific information systems supporting the JTF mission of which the GCCS mission is one facet. The

commanders of the JTF will administer their GCCS assets depending upon the specific mission they are supporting. The office that is typically charged with this responsibility is the JTF Joint Communications Control Center (JCCC) and it functions as the LCC for the JTF. The JCCC has a much broader mission in that it is responsible for managing all systems, not just information systems like the GCCS. The GCCS assets include software (applications, databases, operating systems, etc.) and hardware (clients, servers, management platforms, routers, communication servers, etc.). It is imperative the JTF's JCCC have sufficient levels of expertise to maintain their GCCS assets during deployment. This will range from the manpower necessary to support a few deployed GCCS workstations to the personnel necessary to support a fully deployed GCCS site complete with a data server, application servers, AMHS server, and user workstations. Section 3.4.8.3 identifies those personnel positions that may be required.

4.5 DISA DII RCCs and GCC

The GCC has a unique view of "the big picture" of DISA operated DoD communications. The RCCs are in constant interaction with the DoD user communities, in this case the GCCS community. As a result, the GCC and RCCs are in an excellent position to recommend changes to policies, directives, procedures, and standards that are relevant to GCCS network operations. Additional information concerning the interaction between the DISN RCCs and GCC and the GMC can be found below and in section 4.10.

4.5.1 Monitoring the GCCS Within DISN

The DISN RCCs are responsible for managing, directing, and operating the day-to-day events of the DISN. This includes the SIPRNET which is used as the primary wide area network backbone for the GCCS. The GCCS is a "networked" system using the SIPRNET WAN, the AFC2N WAN, and other CINC unique WANs or communications infrastructures for connectivity. The GCCS "network" includes all equipment, software, circuits, routers, communications servers, WANs, and other S/A communications assets required to interlink the GCCS sites together. While the SIPRNET and S/A and CINC WANs are considered to be an integral part of the GCCS "network", they are not controlled or managed by the GCCS GMC. Likewise, the DII RCCs will have no responsibility for managing GCCS premise routers, GCCS communication servers, or other GCCS network devices. The demarcation point is described clearly in section 2.2.2.

4.5.2 GCCS Enterprise Network, DISN Performance Monitoring

The DISN RCCs are responsible from compiling performance statistics for the SIPRNET. One of the statistics being gathered is the access circuit utilization rates between the SIPRNET WAN routers and the customer's premise routers. Another statistic being gathered is the overall bandwidth utilization of the SIPRNET. This statistic serves as an overall usage indicator of the health of the

SIPRNET. This indicator can be extrapolated to understand the ability of SIPRNET to handle the wartime demands of the GCCS community.

The DISN GCC will make available to the GCCS DIR the bimonthly SIPRNET performance report that is normally produced on the operational performance of the SIPRNET. This report includes, but is not limited to, network traffic loads, throughput, SIPRNET equipment outages, etc. Specific reports concerning the GCCS access circuits to the SIPRNET WAN router will be provided by the DII/DISN RCCs on a monthly basis. These reports will contain the circuit utilization rates, packet drop rates, and delay rates for the access circuits. All reports will be used as the basis for modifying and enhancing the GCCS connectivity to the SIPRNET accordingly.

4.5.3 Problem Management

The DII/DISN RCCs will monitor the DISN networks to detect, isolate, and correct DISN network problems. When problems occur on the SIPRNET that effects the overall health of the GCCS network the GMC-Pentagon office will be notified by the DII/DISN RCCs. The DISN RCCs will coordinate with the GMC-Pentagon on all efforts to detect, isolate, and correct problems associated with the GCCS.

4.6 S/A and CINC WAN Providers

Whereas, the GCC for the DISN has a unique view of "the big picture" of DISA operated DoD communications, the S/A and CINC WAN providers (AFC2N and SCAMPI) do not have the same global view. The management centers for the S/A and CINC WANs' interaction is with their closed community of interest. As a result, the S/A and CINC WAN providers are not in as good as position to recommend changes to policies, directives, procedures, and standards that are relevant to GCCS network operations. However their input will be used to help determine future GCCS requirements

4.6.1 Monitoring the GCCS Within S/A and CINC WANS

The S/A and CINC WAN providers are responsible for managing, directing, and operating the day-to-day events of their network. The GCCS is a "networked" system using the various WANs for connectivity. Again, the GCCS "network" includes all equipment, software, circuits, routers, communications servers, WANs, and other S/A communications assets required to interlink the GCCS sites together. While the S/A and CINC WANs are considered to be an integral part of the GCCS "network", they are not controlled or managed by the GCCS GMC. Likewise, the S/A and CINC management center typically will have no responsibility for managing GCCS premise routers, GCCS communication servers, or other GCCS network devices. However, it may be that a S/A or CINC management center is given the responsibility to oversee and control all GCCS sites underneath their S/A or CINC organization.

4.6.2 GCCS Enterprise Network, S/A and CINC WAN Performance Monitoring

The S/A and CINC WAN providers are responsible for compiling performance statistics for their

networks. The statistics gathered should be the same as those identified in section 4.5.2. The statistics will be used as an overall usage indicator of the health of the S/A and CINC WANs. These indicators will be extrapolated to understand the ability of S/A and CINC WANs to handle the wartime demands of the GCCS community.

The S/A and CINC WAN providers will make available to the GCCS DIR weekly and monthly reports on the operational status of their WAN. These reports will include, but are not limited to, network traffic loads, throughput, WAN equipment outages, etc. Specific reports concerning the GCCS access circuits to the S/A or CINC WAN router will be provided by the S/A and CINC WAN providers on a monthly basis. These reports will contain the circuit utilization rates, packet drop rates, and delay rates for the access circuits. All reports will be used as the basis for modifying and enhancing the GCCS connectivity to the S/A or CINC WAN accordingly.

4.6.3 Problem Management

The S/A and CINC WAN providers will monitor their networks to detect, isolate, and correct network problems. When problems occur on their network that affect the overall health of the GCCS network the GMC-Pentagon office will be notified by the S/A or CINC WAN management center. The S/A and CINC management centers will coordinate with the GMC-Pentagon on all efforts to detect, isolate, and correct problems associated with the GCCS.

4.7 GCCS Management Center (GMC)

The GCCS Management Center (GMC) software and hardware infrastructure at the Pentagon, Site R, and OSF locations will be installed and activated by DISA. The GMC will support the activities of all the GCCS sites, the National Military Command Center (NMCC), and the functions of the JCS/J6 GCCS DIR. The GMC will be operational 24 hours a day, 7 days a week, managing the GCCS, providing operational status to the JCS, and supporting GCCS operations.

The GMC-Pentagon will serve as the primary interface with all the GCCS sites and users for day-to-day operations on the GCCS. The GMC personnel must be proficient in both the system and network management applications, the GCCS joint operational mission applications, and the DII COE components.

The GMC operations will be performed at separate sites as described earlier; each one will have the capability of absorbing all functions in case the others cease to operate with the exception of the GMC-OSF. All Priority-Mode operations, performance management, fault management, and security monitoring will be conducted from the GMC-Pentagon facilities in the Pentagon. The initial GMC-HelpDesk was operated from the GMC-OSF facilities in Sterling, Virginia. The GMC-HelpDesk capabilities for the GCCS migrated to the GMC-Pentagon on 6 June 1996. A third, fully equipped GMC facility will be maintained at Site R, near Ft Ritchie, Maryland, and will have the necessary capacity to totally manage the GCCS. The following sections describe the primary responsibilities to be performed at each GMC location.

4.7.1 Planning and Engineering

The GMC-OSF will be responsible for performing the activities identified in Table 2. The GMC-OSF will receive guidance from the GCCS Engineering Office on how to perform the specific engineering duties while receiving operational management direction and guidance from the GMC-Pentagon. Based on information gathered on the GCCS, the GMC-OSF will make planning and engineering recommendations to the GCCS DIR on ways to improve the operational capabilities of the GCCS.

4.7.2 Management

The GMC-Pentagon will be responsible for performing the activities identified in Table 3 with two exceptions. The GMC-OSF will be responsible for the Provisioning and Logistics functions identified in Table 3. The GMC-Site R will act as a backup for all activities performed by the GMC-Pentagon.

4.7.3 Operations

The GMC-Pentagon will be responsible for performing the activities identified in Table 4 with one exception. The GMC-OSF was initially responsible for the GMC-HelpDesk functions identified in Table 4 until that capability was migrated to the GMC-Pentagon. The GMC-Site R will act as a backup for all activities performed by the GMC-Pentagon.

4.7.4 GMC-HelpDesk

The GMC-HelpDesk is the GCCS user's primary point of contact for all problems associated with the joint mission pertaining to hardware, software, network, or communications. The GMC-HelpDesk will not be responsible for supporting CINC or S/A unique applications. Any user may report a problem; however, the user should coordinate with the GCCS Site Coordinator to verify a problem really exists prior to contacting the GMC-HelpDesk. The GCCS Site Coordinator should make every effort to resolve the problem at the local site using resident operations and maintenance personnel before escalating the problem to the GMC-HelpDesk. The GMC-HelpDesk tracks problems from identification and notification to resolution and will be the only trouble ticketing system within the GCCS supporting the joint environment. It will keep each GCCS Site Coordinator informed of the status of any trouble tickets open against their site. The GMC-HelpDesk will accomplish this function through the use of procedures and system and network management tools. The procedures and tools provide essential support functions for effective network, system, and administrative management, thus providing a vital link between users and technology. GMC-HelpDesk trouble tickets will use predefined codes for tracking. The automated tools or GMC technicians will assign priorities for each trouble ticket along with the projected estimated time of repair (ETR) when possible. Gathering and recording all information available about problems on the GCCS, to include hardware, software, and data related, will be one of the major tasks of the GMC-HelpDesk. The building of the knowledge base at the GMC-HelpDesk will take time. However, industry standards show in practice that a knowledgeable Help Desk can resolve over 75% of problems using the knowledge base and case histories on the first call without additional support. The remaining

problems usually require hardware repair, advanced technical or engineering knowledge, or problem escalation to another provider.

The GMC-HelpDesk operates twenty-four (24) hours a day, seven (7) days a week at the GMC-Pentagon, effective 6 June 1996. The GCCS users were notified of this change by formal message from Joint Staff Washington DC, DTG 292030Z May 96, Subj: Global Command and Control System Management Center (GMC) Help Desk Activation. The message was sent to the GCCS Address Indicator Groups (AIGs) of 8785, 8786, 8787, and 8791. The information was also broadcast on the GCCS.GMC.HELP NewsGroup.

As stated earlier, the GMC-HelpDesk is the GCCS user's primary point of contact for all problems associated with the joint mission which cannot be resolved locally. It is important to stress that the GMC-HelpDesk will be for the secret level GCCS users initially. A residual WWMCCS staff provides help desk support for the TS3 top secret portion of the GCCS. Once the planned upgrade of TS3 to the GCCS(T) has occurred, the same hardware and software approach used by the secret level GCCS will be mirrored to support the GCCS(T). Once this happens there will be a single GMC-HelpDesk supporting both classification levels. The GCCS(T) users will be notified of this change by formal message to the GCCS AIGs. The change in procedure also will be posted on the secret level GCCS.GMC.HELP NewsGroup.

Most of the CINC locations and the S/As are setting up their own helpdesk functions. For a GCCS site there may be a hierarchy of helpdesks before they reach the GMC-HelpDesk. It is important that problems be resolved at the lowest possible level while still keeping all levels informed. For this reason it is imperative that the GMC locations have a view into any CINC or S/A helpdesk supporting the GCCS. Likewise, GCCS users must have a view into the GMC-HelpDesk.

The GMC technicians in support of the GMC-HelpDesk functionality will provide technical assistance to all GCCS sites and users. Specific tasks performed by the GMC technicians to support the GMC-HelpDesk will include, but are not limited to the following:

- Maintaining component inventory management to track problems against hardware or software
- Maintaining parent-child relationships or dependencies between components or segments
- Maintaining trouble ticketing system to provide problem history
- Maintaining vendor/maintenance responsiveness history

- Problem status escalation to higher levels (interfacing with DII/DISN RCCs and S/A and CINC WAN management centers)
- Monitoring machine generated trouble tickets (trouble tickets are automatically generated when system events occur due to network management integration)
- Providing centralized problem management and information services (for troubleshooting network operating software, system operating software, GCCS

application software, all GCCS hardware, and GCCS security problems)
- Archiving of problems/trouble tickets for future reference
- Interfacing to GCCS.GMC.HELP NewsGroup to distribute system advisory notices to users
- Interfacing to user's e-mail to create trouble tickets
- Interfacing to web server to create trouble tickets
- Interfacing with users to query status of trouble tickets via secure e-mail
- Interfacing to user's telephonically

4.7.4.1 System and Network Management

The GMC-Pentagon will be the center of all system and network management activities for the GCCS. Two of the critical functions performed by the GMC-Pentagon are the monitoring of the GCCS and the collection of performance data on the total GCCS as well as individual components. However, the Site R locations will receive the smart agent data real-time also to ensure survivability of the joint management function.

4.7.4.2 Monitoring the GCCS

The GMC-Pentagon will monitor the entire GCCS infrastructure (including the SIPRNET and other S/A and CINC WANs via exchanged management data) to detect, isolate, and when possible correct GCCS system or network related problems. Monitoring of WANs and communications infrastructures outside the scope of the GMC and GCCS sites will be through the exchange of peer-to-peer management data explained in section 4.9. Though the GMC-Pentagon will be able to view the SIPRNET and other S/A WANs status, it will not have operational control of these WANs. The GMC's role will be to assist WAN service providers during the troubleshooting process if asked to do so. WAN management and troubleshooting is the responsibility of the DII/DISN RCCs or designated S/A and CINC management centers of that network. The GMC-Pentagon will coordinate all detection, isolation, and corrective activities with the local GCCS sites, the DII/DISN RCCs and GCC, and any other S/A whose assets may be at fault.

During routine operations the GMC will limit itself to advising and assisting the local GCCS sites. During Priority-Mode operations, all GCCS sites management functions will be subordinated to the GMC-Pentagon, through the J3 DICO.

4.7.4.3 Performance Monitoring

The GMC-Pentagon will be responsible for compiling performance statistics for the entire GCCS. Some statistics that will be gathered are the GCCS premise router to WAN router access circuit utilization rates, data and application server failure rates, and AMHS availability rates. Other statistics classified as mission essential by the GCCS DIR will also be gathered.

The GMC-Pentagon will use automated monitoring software (smart agents) and devices at each GCCS site to assist in the collection of performance data. In addition, the GMC will record outages and other vital information as reported by each GCCS Site Coordinator not previously trapped by the automated software. Between the two capabilities, the complete picture of the GCCS should be available at the GMC.

The GMC-Pentagon will provide to the GCCS DIR daily, weekly, and monthly reports. These reports will include, but not be limited to, network traffic loads, throughput, site outages, network bottlenecks, etc. The reports will be used to modify and enhance the GCCS network accordingly.

The GMC-Pentagon will provide each site with a monthly report on the performance of their site as seen from the GMC. The site will use this report to ensure its operation meets and maintains the level of performance required by the GCCS Network.

The GMC-Pentagon will maintain historical data on network performance and utilization and will publish an annual report analyzing past versus present performance.

Developmental work is underway to see how these reports can be posted onto a web site so GCCS sites can access this data also. The goal will be to eliminate hardcopy, paper reports from the management structure.

The specifics of performance criteria and thresholds will be published in a separate document to be produced by the GCCS Engineering Office. This document will be titled the *Global Command and Control System (GCCS), Performance Criteria and Measurement Thresholds*. This document will be published by GMC FOC.

4.7.4.4 Trouble Ticketing Systems

4.7.4.4.1 GCCS Trouble Ticketing System

The GCCS will use an automated trouble ticketing system available to all users but centrally administered by the GMC-HelpDesk. Any user may report a problem; however, the user should coordinate with the GCCS Site Coordinator to verify a problem exists prior to generating a trouble ticket. Each trouble ticket will contain only one (1) problem to be resolved. The system is the Action Request System (ARS) by the Remedy Corporation. The Remedy ARS is a highly flexible system based on the open system environment that can be used across the entire spectrum of the GCCS for reporting troubles. One of the major benefits of Remedy ARS is that trouble tickets can be generated automatically by other intelligent system and network management software applications running at the GMC.

The trouble ticketing system application is unclassified. However, the actual trouble tickets may be classified if they describe events which security policies and documents deem classified within the GCCS. All initial trouble tickets will be considered system high (i.e. Secret), until they can be

reviewed by the GMC technicians and assigned the proper classification based on the security classification documents. All trouble tickets will contain a classification field for this reason. An example of how a classified trouble ticket could exist follows. Initially, one of the network management software applications operating at the GMC detects that a GCCS premise router has failed at one of the sites and the site no longer has WAN access. The network management software application automatically generates a Remedy ARS trouble ticket stating that the GCCS site is off the network. Using a predefined events table, the Remedy ARS knows that the event where a GCCS site has lost network connectivity is classified as secret. A secret level trouble ticket is generated and the GMC technician is notified of the critical event. In most cases, trouble tickets for events of this nature will be generated before the GCCS site or the GMC technician even are aware that a problem has developed somewhere within the GCCS.

Remedy ARS can support a multitude of different databases for storing trouble tickets. One of the databases supported is the existing GCCS database standard (Oracle). As such, Oracle will be the database that will be used to support the Remedy ARS. Two Remedy ARS database engines will be installed on the GCCS. One will be at the GMC-Pentagon and the other at the GMC-Site R using the GMC servers. While there are two engines, the two sites will utilize mirrored sets of data. The GMC-Pentagon will be the active site with backups made to the GMC-Site R location.

Interaction with the Remedy ARS can occur from a multitude of locations throughout the GCCS. However, the GMC-HelpDesk will be the focal point for coordinating all joint GCCS trouble tickets. The GMC-HelpDesk will have three major tasks in relation to the trouble ticketing system. The first will be to assign the Priority field based on Appendix C of MIL-STD-498, *Software Development and Documentation*, 5 December 1994. The GCCS end users will not be able to assign the Priority field. This function will be kept at the GMC-HelpDesk to ensure MIL-STD-498 is followed properly. However, GCCS Site Coordinators will assign the Site Impact field to show the criticality of the problem at the site. The second major task will be to ensure the trouble tickets are passed to the proper organization or person for corrective action. The third major task will be to ensure the Classification field is appropriately assigned for each trouble ticket. GMC technicians will be able to generate trouble tickets, query the trouble ticketing database for a variety of purposes, and closeout and transmit responses concerning trouble tickets in the Remedy ARS. GCCS end users also will have the ability to generate trouble tickets from their GCCS workstation. They can query the trouble ticketing database to see if the problem they are experiencing has previously occurred within the GCCS prior to submitting a trouble ticket. They can also view the status of an outstanding trouble ticket previously submitted. Additionally, after a problem has been resolved they can look into the database to see what corrective action was taken. Figure 22 is representative of the typical flow of trouble tickets from problem identification through problem resolution. The drawing does not show all of the many intermediary steps that must occur in the troubleshooting process. All trouble tickets not immediately solved at the GMC-HelpDesk will be escalated to the appropriate expert or developer for resolution. If the problem seriously impacts mission essential capabilities, a temporary "work around" may be developed and used until the problem can be permanently resolved. Proposed work arounds and final solutions will undergo a quality control check through product assurance testing before being accepted. Accepted software solutions or software patches will be incorporated

in the baseline of the next major GCCS software release.

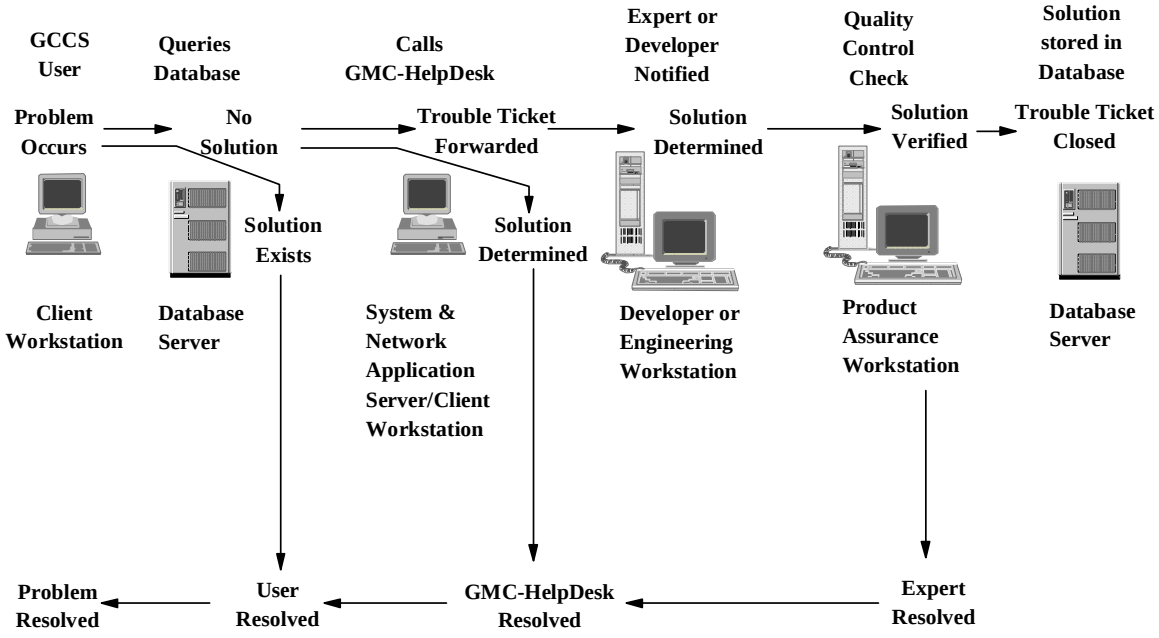


Figure 22 Trouble Ticketing Flow

The final area of interaction with the Remedy ARS will be from the network and system management software operating on the GCCS. The intelligent COTS software will be programmed to automatically generate trouble tickets based on certain events occurring as defined in a rules table. For these automatically generated trouble tickets the GMC technicians will not assign the Priority field, Site Impact field, or Classification field. These fields will be contained in management rule tables and will be inserted automatically upon generation of the trouble ticket. Figure 23 shows the Remedy ARS and its underlying database along with the various sources that interact with the system.

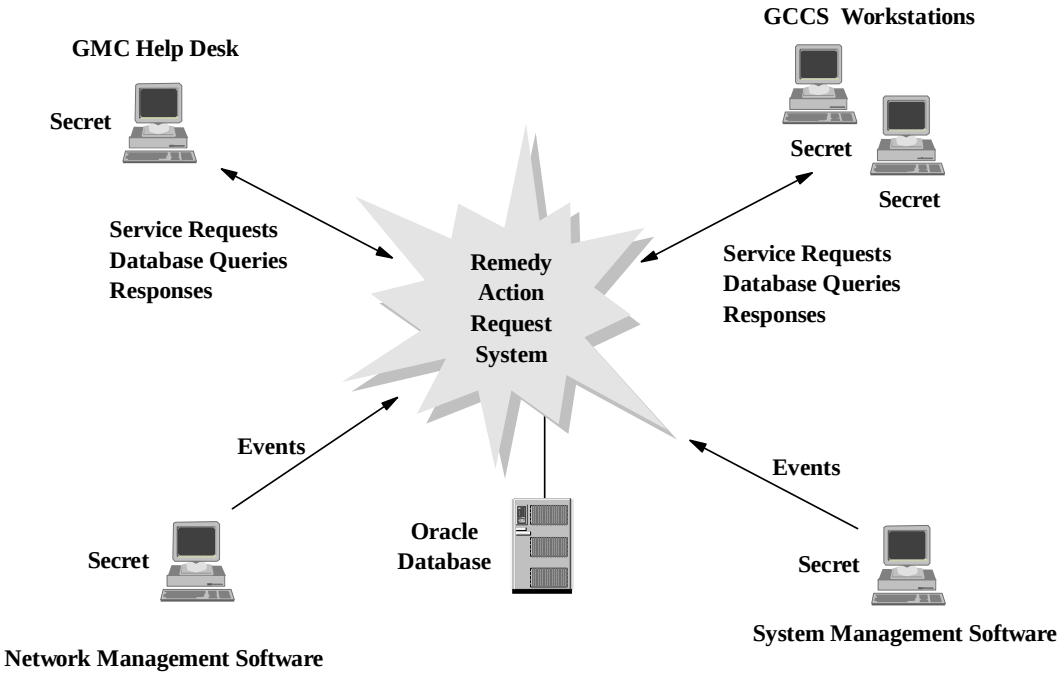


Figure 23 Interrelationship of Remedy ARS and the GCCS

The deployment of Remedy ARS will occur in three phases. The first phase will be to install the Remedy ARS system at the GMC-Pentagon and GMC-Site R locations and get the trouble ticketing database structure established. The second phase will be to educate the GCCS Site Coordinators and GCCS System Administrators at each primary GCCS site on the Remedy ARS and how to use it. The final phase will be to educate all GCCS users on how to perform trouble ticketing functions from their GCCS terminal. During the first phase, the GMC technicians will log and maintain all trouble-tickets for the GCCS. In the second phase the GCCS Site Coordinators, the GCCS System Administrators, the GCCS Network Administrators, the GCCS Database Administrators, and the Site GCCS Information System Security Officers will also be able to enter trouble tickets electronically into the system. The final capability is achieved during phase three when all GCCS users will have the ability to submit trouble tickets electronically to the GMC-HelpDesk. No timetable has been established for phase two or phase three.

A parallel effort to the three phase Remedy ARS implementation will be to program the intelligent network and system software applications to automatically generate trouble tickets. No timetable has been established for this effort but it relies on several factors. The first factor is the smart agents deployed and reporting from all GCCS sites. The second factor is a smart manager installed at the GMC reacting to the traps and reports sent in from the field by the smart agents. The third step is to have the smart manager perform a correlation function to take multiple events and traps and reduce

that to the root cause of the problem. The fourth factor will be to define the rule sets for how the trouble tickets will be automatically generated. This will be the most involved and intense activity of the automated process. And finally, the programming of the smart manager such that the autogenerated ticket occurs.

The DISA/WESTHEM/JSSC, responsible for the GMC-Pentagon, in conjuction with the DISA GCCS Engineering Office will produce additional documentation outlining the policies and procedures of the trouble ticketing system. For additional information contact the GMC-HelpDesk.

4.7.4.4.2 Non-GCCS Trouble Ticketing Systems

GCCS users will reley on the Remedy ARS at the GMC-Pentagon for information concerning the GCCS. In addition, there are other trouble ticketing systems that will be important for the GMC to have access to. For example, there is a Remedy trouble ticketing system used by the DISN GCC and RCCs to document DII networks. It will be important for the GMC-Pentagon to have access to this system so they can have access to the health and welfare information of the SIPRNET. The detail of this access will be worked out between the GMC-Pentagon personnel and the DISA/D3 operations personnel. Another trouble ticketing sytem that will be important to the GMC-Pentagon is the DII COE trouble ticketing system and the GCCS developmental software trouble ticketing system. Both of these systems are at the DISA OSF building and are used for internal tracking of software problems. A view into these systems at the GMC locations will provide valuable troubleshooting data to the GMC-HelpDesk personnel. Most of the CINCs and Services are standing up trouble ticketing systems. A sharing of the views of the various troubleticketing systems will help keep all informed of the health of the GCCS. Specific details and implementation practices and procedures will have to be worked out for the interaction between all the different troubleticketing systems.

4.7.5 GMC Functional Areas

Each functional component performs its functions through one or more of the International Standards Organization's (ISO) Functional Management Areas (FMA). The five FMAs are Fault, Configuration, Accounting, Performance and Security Management. The ISO model for management applies the FMAs concepts to both network and system management. The GMC will employ a system management perspective for the overall GCCS and a network management perspective for the individual GCCS sites and their campus components. Network management of the various WANs supporting the GCCS will be by the management organization responsible for these networks. The remainder of this section will discuss the functions of the GMC using the ISO FMA as filters. The FMAs permeate throughout the GMC Functional Components.

4.7.5.1 Configuration Management (CM)

The GMC will maintain a configuration management system to track configuration elements. The GMC will be assisted by site GSC, GNA, and GSA personnel in ensuring the accuracy of the data. The following configuration management elements will be tracked as a minimum:

- GCCS Hardware Configuration
- GCCS Software Configuration
- GCCS Network Configuration
- Site specific hardware, software, and network configuration information
- Inventory Control to include spare equipment management
- Host and Domain Names
- IP Network Addressing

The Accugraph Physical Network Management Bundle will be used to provide the graphical picture of the GCCS. In essence, this application will provide a series of drawings of the entire GCCS infrastructure. Included in the drawings will be all GCCS primary sites, secondary sites, remote users, and other supporting Non-GCCS infrastructures. These graphical pictures will be the primary display for the workstations at the GMC locations. GSC, GNA, and GSA personnel at the GCCS sites are tasked to review the drawings representing their sites monthly to ensure accuracy of the drawings.

The Accugraph product has a linked, underlying database. With this database one can tell how many Sun Sparc 5/85s are operating on the GCCS. Another example could be that one can print out the entire list of GCCS remote users to include their location, the hardware they use, and the communications paths linking them to GCCS capabilities. The data that can be provided is limited only to the scope and depth for which the linked database is programmed and populated.

The Accugraph Physical Network Management Bundle supports the existing GCCS database standard (Oracle). As such, Oracle will be the database that will be used to support the network application. Two Accugraph database engines will be installed on the GCCS. One will be at the GMC-Pentagon and the other at the GMC-Site R using existing GMC servers at those sites. Again, like the Remedy ARS, while there are two engines, the two sites will utilize the same set of mirrored data. The GMC-Pentagon will be the active site with backups made to the GMC-Site R location. The Accugraph drawings will contain an icon for every physical entity on the GCCS. The *Global Command and Control System (GCCS), System and Network Management, Implementation Plan* will contain an appendix that is library of all icons used with the GMC drawings. There will be a one type of icon per drawing item. For example, a Sun Sparc 5/70 would be represented differently than a Sun Sparc 5/85. Additionally, each icon will be color coded based on its current state. A green icon will represent a device that is fully operational. A red icon will represent a totally failed device. An orange icon will represent a device that is on the verge of failure based on a predefined performance events table. A yellow icon will represent a device that has triggered a performance event from a predefined events table that is not deemed critical. Finally, a purple icon will represent a device that is functional, but inoperative due to a higher order failure. An example of this would be a communications server attached to a router by a single serial connection. If the router had failed it would be represented by a red icon. The communications server is still operational but can not pass traffic through the router due to the communications circuit failure. It would be represented by a purple icon.

A pending developmental effort will provide the software configuration of each GCCS hardware platform. The SAInstaller will be modified in a future release to build a file on each hardware

platform that lists which segments and versions are loaded on that platform. This file is continually modified as segments are added, deleted, or upgraded on that platform. This file will be linked to the specific machine based on its IP address and host name which are unique across the entire system. This file containing the software load will be copied from each platform to the Accugraph database on a periodic basis. Thus the database will contain the software configuration for each GCCS platform.

GSC, GNA, and GSA personnel at the GCCS sites will be responsible for reviewing their site drawings monthly as discussed previously to ensure the drawings accuracy. However, changes in IP addresses, domain names, host names, communications connectivity, etc. should be communicated to the GMC-Pentagon as quickly as feasible. Preferrable before the change is to take effect or worst case, within 24 hours of activation.

4.7.5.2 Security Management (SM)

The GCCS operates in the System High mode of operation and processes up to secret information. The TS3 and future GCCS(T) also operate System High processing information at the top secret level. The GCCS security policy statements comply with governing security regulations to ensure the GCCS operates in a secure manner while using, storing, or distributing sensitive information. Operational success of the GCCS depends on the system accurately providing four security services. They are:

- Accountability. Ensuring that activities performed on the GCCS can be traced to individuals who then may be held responsible for their actions.
- Availability. Ensuring the system, network, and information is accessible and usable upon demand by an authorized GCCS entity. The network includes sites LANs, WANs, and other supporting communications systems.
- Confidentiality. Ensuring that information is not made available or disclosed to unauthorized individuals, governments, entities, or processes.
- Integrity. Ensuring that C2 system and network integrity along with the C2 information has not been altered or destroyed in an unauthorized manner.

The GMC will maintain a security management function to perform the tasks listed below. Some of the specifics of how these tasks will be accomplished are being defined. The tasks are:

- Password management by the ISSO to give each user unique User Id and password
- GCCS Executive Manager application provides login/logout menus
- Access control across the GCCS organization
- Identify/maintain secure access points to the secret LAN/WAN structure
- Identify/maintain sensitive information using appropriate controls
- Identify security breaches through automated attack and search tools
- Maintain the automated attack and search tools (GMC-Pentagon location)

No COTS software package will be used to perform SM for GCCS Version 2.1 or 2.2 software releases. SM is performed by the GOTS packages internal to the GCCS COE. Future releases of GCCS software versions may include COTS products to perform additional security functions.

4.7.5.3 Fault Management (FM)

A variety of COTS packages are used for FM. Some of the initial COTS applications identified for use at the GMC were identified in section 3.4.7.2. The only GOTS product to be used at this time is the GCCS System Services application. FM relies heavily on the tools installed at the GMC locations being able to reach out across the WANs to access the GCCS sites via SNMP. This is one of the many reasons why SNMP must be enabled on all devices supporting the WANs and the GCCS LANs.

The applications identified in section 3.4.7.2 will be configured to provide critical event reporting on network problems, server failures, malfunctioning GCCS applications, etc. It will take time to determine which specific events are deemed critical and which are less severe. It is expected that during the first year of operation of the GCCS a large degree of fine tuning of these applications will be required.

4.7.5.4 Performance Management (PM)

The GMC will use the same COTS and GOTS tools identified previously to perform the PM role. The tools will be used to track the following parameters as a minimum:

- Bandwidth utilization, packets drop rates, and end-to-end performance on access circuits
- Access circuit availability
- LAN utilization rates by protocol
- Input/Output utilization rates
- Hard disk utilization rates of application and data servers
- CPU utilization rates of application and data servers
- AMHS utilization rate of AUTODIN feeder circuit

The requirements for PM will be based on a multitude of parameters associated with acceptable levels of performance. The collecting of the statistical information will be used to analyze system and network utilization trends. Again, it will take time to determine which specific parameters are needed to do the analysis. Again, it is expected that during the first year of operation a large degree of fine tuning of these parameters will take place. For example, the utilization threshold for the router access circuits initially will be set at 50 percent. This will show the GMC-Pentagon which GCCS sites are using more than half of their available bandwidth. If a GCCS site is using more than 50 percent available bandwidth, then the GMC-Pentagon will recommend to the site to lease a larger WAN access circuit to allow for wartime growth. With time it might be determined that the 50 percent factor be changed to a 60 percent threshold and still meet the wartime needs of the site. The PM functionality will aid greatly in optimizing the system and network performance of the GCCS.

The key component of PM is the smart agents deployed at the GCCS sites. These agents are the heart of the statistical collection effort. Without their being in place the health of a location is based on a subjective and not an objective data analysis. Again, these smart agents use SNMP to send their statistical reports to the GMC locations. This is another of the many reasons why SNMP must be enabled on the WANs and GCCS LANs devices.

The Joint Staff has tasked DISA to provide oversight management as to the health and welfare of the GCCS. DISA/WESTHEM/JSSC accomplishes this mission by operating the GMC-Pentagon and GMC-Site R locations. It is mandatory the smart agents report to these two locations so DISA can fulfill it oversight management role for the Joint Staff. The DISA GCCS PMO will fund and provide the smart agents for installation at the GCCS sites to meet this role. However, this is only the smart agents. It does not include any system and network management hardware or software that the sites may need to manage themselves. This is the responsibility of the S/A GCCS PMOs in accordance to S/A policy as previously stated in section 3.4.5.2. Further information is included in sections 3.4.7.5 and 4.11 concerning the smart agents.

4.7.5.5 Accounting Management (AM)

The functions associated with AM are not deemed critical for the GCCS to go operational. A large portion of AM is associated with charge-back procedures for which GCCS has no requirement at this time. The GCCS does not resell or time share system assets with non-GCCS subscribers. The GCCS sites pay the DISN SIPRNET based on the bandwidth size of the router access circuit, not on usage like the DDN. The monthly bill will not change if the GCCS must surge to support a crisis or contingency somewhere in the world unless the GCCS site changes to a larger router access circuit. The pricing systems for the other S/A and CINC WANs may charge differently. Some of the functionality of AM includes cost analysis and trends associated with maintaining a system. This functionality will be examined in greater detail to see how implementing it would help the GCCS community. It may become a very valuable tool for the logisticians and financial officer responsible for the funding issues associated with the GCCS.

4.7.6 Software Releases, Installation and Cutover Coordination

This section provides specific procedures for the installation of and cutover to new releases of GCCS software. The GCCS uses a complex collection of software applications to perform the overall joint C2 mission. These joint applications are divided into the following categories: kernel, common operating environment (COE), common applications (predominant COTS packages), and mission applications. The COE is further sub-divided into standard COE and “embedded user functionality”. The latter are applications that provide functions required for users to do their jobs, and have a significant impact on how users do their jobs. In addition, a GCCS site may have other software applications loaded that are unique CINC or S/A mission requirements at that particular location. This section will pertain to the joint applications. It will be the responsibility of the individual CINC or S/A to determine their procedures for loading new applications. However, the CINC or S/A still must coordinate their unique installation and cutover schedule with the GMC since it may effect the

site's war readiness condition.

Each of the applications in the categories described above are composed of segments. Some of these segments are both site-interdependent as well as site-independent. There is not always a clear separation between these two groups, which results in GCCS software generally being classified as site-interdependent. To assure that problems with the GCCS software can readily be predicted, diagnosed, and resolved, the installation of changes to GCCS software will be controlled by the GCCS DIR as the designated Configuration Manager for the GCCS.

The GMC-OSF, operated by the DISA Center for Computer System Engineering, will be responsible for electronically distributing, coordinating, and testing all new GCCS applications software releases. In addition, the GMC will participate materially in GCCS Standard Software pre-release testing and evaluation and provide recommendations as appropriate.

4.7.6.1 DII COE Software Definitions

The following are a few definitions from the DII COE Integration and Runtime Specification (I&RTS) that are commonly used GCCS software terms:

- Aggregate Segment: A collection of segments grouped together, installed, deleted, and managed as a single unit

- Application Programmer Interface (API): A programmer's guide that describes the COE software libraries and services, and how to write software modules that interface with and use the COE services.

- Approved Software: Software that has been tested as compatible with the COE. An approved products list might contain Oracle, Sybase, WordPerfect, Kermit, SEWC, NITES, etc. In this context, approved software implies only that the software has been tested and confirmed to work within the environment. It does *not* imply that the software has been approved or authorized by any government agency for any specific system.

- Bootstrap COE: That subset of the COE that is loaded in order to have enough of an operational environment that segments can be loaded. The bootstrap COE is typically loaded along with the operating system though vendor supplied instructions or low level Unix commands a such as *tar* and *cpio*.

- Client: A computer program, such as a mission application, that requires a service. Clients are consumers of data while servers are producers of data.

- Common Operating Environment (COE): The architecture, software infrastructure, core software, APIs, runtime environment definition, standards and guidelines, and methodology required to build a Command Information System. The COE allows segments created by

separate developers to function together as an integrated system.

- Compliance: A numeric value, called the compliance level, which measures the degree to which a segment conforms to the principles and requirements defined by COE standards, and the degree to which the segment makes use of COE services. Compliance is measured in four areas, called compliance categories. The four categories are Runtime Environment, Architectural Compatabiltiy, Style Guide, and Software Quality.

- Distributed Database: A database whose data objects exist across multiple computer systems or sites.

- Distributed Processing: The ability to perform collaborative processing across multiple computers. This capability allows processing load to be distributed.

- Environment: In the context of the COE, all software that is running from the time the computer is rebooted to the time the system is ready to respond to operator queries after operator login. This software includes the operating system, security software, installation software, windowing environment, COE services etc. The environment is subdivided into a runtime environment and a software development environment.

- Kernel COE: That subset of the COE component segments which is required on all workstations. As a minimum, this consists of the operating system, windowing software, security, segment installation software, and an Executive Manager.

- Mission Area Variant: A collection of segments which are relevant to a particular mission area (e.g., Analysis, Planning). A mission area variant is typically a list of workstation variants.

- Remote Install: The ability to electronically install segments from a local site (such as the DISA Operational Support Facility) to a remote site (such as USACOM). In a “push” mode, the local site initiates and controls the segment installation. In a “pull” mode, the remote site initiates and controls the segment installation.

- Runtime Environment: The runtime context detemined by the applicable account group, the COE, and the executing segments.

- Segment: A collection of one or more CSCIs (Computer Software Configuration Items) most conveniently managed as a unit. Segments are generally defined to keep related CSCIs together so that functionality may be easily included or excluded in a variant.

- Site Variant: A collection of segments that are relevant to the mission needs of a specific site (e.g., CVN, TRANSCOM, CJTF). A site variant is typically a list of mission area variants.

- System Variant: A collection of segments that are relevant to a specific defined mission area (e.g., C4I, logistics, finance). GCCS and GCSS are two examples of a system variant. A system variant is typically a list of site variants.

- Variant. A subset of the superset of all software. This subset includes the COE, and is fielded to service an operational mission area. A variant represents that collection of segments, including COE component segments, that are suitable for a particular site, mission area, or workstation. See also the definiton of mission area, site, system, and workstation variants.

4.7.6.2 Responsibilities

The GCCS DIR will perform the following functions:

- Monitors and coordinates the implementation of GCCS releases to minimize any possible adverse operational impact on the GCCS. Releases could range from the total replacement of GCCS applications to installing a patch that effects only one segment.
- Coordinates the cutover to new GCCS releases, applications, and updates with the affected GCCS sites.
- Acts as the Configuration Manager for the GCCS and coordinates updates to the GCCS within the Joint Staff and with the DISA/JIEO GCCS Engineering Office. Configuration Manager duties include configuration control of the software, hardware, and the GCCS infrastructure.

The DISA/JIEO GCCS Engineering Office will perform the following functions:

- Directs the integration, evaluation, and quality-assurance testing of GCCS application software.
- Recommends release installation and cutover procedures and dates.
- Provides direction on software configuration control of the GCCS software through engineering decisions. The GMC-Pentagon will be responsible for keeping a database of the software configuration of each GCCS server and workstation via the Accugraph COTS product.
- Provides operational support to the GCCS DIR, the GMC, and the GCCS sites in the installation, test, and cutover to any updates made to the operational GCCS baseline software configuration.
- Oversees tests and quality assurance procedures performed by DISA Center for Integration personnel.

The GMC-Pentagon will perform the following functions:

- Provides real-time interface with the GCCS sites on problems and procedures in the installation of GCCS releases and application or segment updates.

- Notifies the GCCS DIR and DISA/JIEO GCCS Engineering Office of all identified problems with the software installations or cutovers.
- Coordinates the installation of software updates to the GCCS applications.
- Provides software configuration control by keeping a database of the software configuration of each GCCS server and workstation via Accugraph.

GCCS sites will perform the following functions:

- Advises the GMC-Pentagon of receipt of GCCS releases/updates as identified in the release/update documentation.
- Complies with installation and cutover instructions provided with the release/update documentation.
- Notifies the GMC-Pentagon of any problems associated with the installation of GCCS releases and application or segment updates.
- Notifies the GMC-Pentagon upon successful completion of the GCCS release/update installation using the reporting procedures described in section 4.7.6.3.

4.7.6.3 Installation Procedures

The following are procedures for the installation of GCCS releases and application or segment updates on the GCCS.

DISA/JIEO will produce GCCS releases and application or segment updates for the joint GCCS applications with accompanying documentation. The general content of each release will be coordinated with the GCCS DIR, the GMC-Pentagon, and by the GCCS Engineering Office. JIEO, in coordination with the GCCS DIR, will prepare a message to AIGs 4503, 8785, 8787, 8786, and 8791 that announces the contents of the release and application or segment updates. This message will also be repeated or referenced in the GCCS.GMC.HELP NewsGroup.

DISA/JIEO will determine the distribution procedures for each GCCS release and application or segment updates. A determination will be made on whether to distribute the software updates electronically across the SIPRNET and the S/A and CINC WANs or if the software will be distributed on 8mm or 4mm magnetic tape via registered mail. The decision will be based on the amount of software code that must be distributed. The software code will be distributed to each Site GCCS ISSO in accordance with approved security practices and policies.

The GCCS DIR, through the GMC-Pentagon, will coordinate installation of each GCCS release and application or segment update with all GCCS sites. Changes to release installation instructions and schedules must be approved by the GCCS DIR.

Coordinated cutovers are made for the purpose of installing GCCS software that is site interdependent, and as such can affect the performance of the entire system if a single GCCS site fails to comply with the installation instructions. Therefore, it is critical that each GCCS site install the

GCCS release and application or segment update on the date and time specified in the cutover message. When it is not possible to cutover within the specified window a waiver must be requested from the GCCS DIR. Three important rationales exist on why the cutovers must occur within the specified window.

- Incompatibility between GCCS releases and application or segment updates may require a coordinated phased cutover requiring that no transmissions occur between those sites which have completed the cutover and those sites that are waiting to cutover. In the WWMCCS, it was not uncommon for the access circuits to the packet switched nodes of DNSET2 to be put into a maintanence loopback to prevent data transmission. This is an outdated concept for today's TCP/IP data networks. The GCCS LANs support many more systems that just the GCCS. It is unacceptable for mission survivability to block the WAN access circuit. In order to maximize the segregation of those sites that have cutover, it may be necessary to stop the transmission of data between GCCS sites. This should be accomplished by "freezing" the application across GCCS and not blocking the access circuits. This is the most severe cutover option and this criteria will be identified in the cutover message.

- Changes to GCCS applications performing the JOPES functionality may require the database servers supporting JOPES applications be brought to zero flow. Zero flow operations of the JOPES databases minimizes the possibility of corrupting the existing data during updates. In essence, JOPES is placed off-line in idle until the software updates are completed. The cutover message will identify if this criteria is in effect.

- It is vital that cutover occur as rapidly as possible to minimize the disruption of GCCS operations. Specific cutover actions and times by GCCS site will be provided by the GCCS DIR in the cutover message.

Non-coordinated cutovers are usually for the installation of GCCS releases and application or segment updates that are not site-interdependent. Each GCCS site will install the software by the specified time. Completion is normally at the site's convenience within guidelines established by the GCCS DIR, based upon the recommendation of DISA GCCS Engineering Office and Joint Staff/J-3.

GCCS sites will notify the GMC-Pentagon immediately following either a coordinated or non-coordinated cutover IAW section 4.6.12.3. The GMC-Pentagon will notify formally the GCCS DIR and the DISA GCCS Engineering Office when the software cutover is complete.

4.7.7 Security

The GMC will monitor network security and will report incidents to the Joint Staff GCCS Security Officer and the GCCS DIR. The GCCS DIR, through the GMC-Pentagon, will notify sites via secure communications of vulnerabilities and corrective measures to be taken to correct deficiencies within the GCCS. Specific tools and practices are still being identified. When necessary, the GMC-Pentagon will be responsible for activating support from the DoD Automated Systems Security

Incident Support Team (ASSIST). The ASSIST provides a centrally coordinated response to incidents anywhere, anytime, and to any one in DoD for resolution of security incidents.

4.7.8 Policies & Procedures.

The GCCS DIR will be responsible for creating, changing, and deleting system and network management policies and procedures. The GCCS DIR may delegate this responsibility on a case by case basis to other organizations depending on the policy or procedure being worked. The GMC-Pentagon will be responsible for the dissemination of changes in GCCS policy or procedure.

4.7.9 Communications with the GMC

The offices of the GMC can be contacted by telephone. Each GMC location will be equipped with STU-IIIs for secure voice. Additionally, each location will support secure and unclassified FAX transmissions. Sufficient telephone lines against a rotary hunt group telephone number will be installed to ensure proper voice coverage at the GMC locations. DSN/AUTOVON and commercial numbers are provided for the GMC locations in the following table. (*) The TS3 telephone numbers will cease to exist once GCCS(T) is operational and being supported by the GMC-Pentagon.

Location	Voice (DSN)	Voice (Commercial)	UNCLASS FAX (DSN)	SECURE FAX (DSN)	Beeper (Commercial)
GMC-Pentagon	225-0671	(703) 695-0671	224-9082	225-0025	N/A
GMC-Site R	988-3136	(301) 868-3136	988-3257	988-3552	N/A
GMC-OSF	653-8681	(703) 735-8681	653-8685	TBD	N/A
GMC-HelpDesk	225-0671	(703) 695-0671	224-9082	225-0025	N/A
TS3 ** (WWMCCS Infrastructure)	225-3025	(703) 695-3025	227-3352	TBD	(202) 773-6965

Table 8 GMC Telephone Directory

The GMC can be contacted by secure e-mail. The GMC mail account will be located at the GMC-Pentagon site. The e-mail account is GMCHELP@GMC.NMCC.SMIL.MIL. A temporary account has been set up at the NMCC site and is DJ9HELP1@NMCC20A.NMCC.SMIL.MIL. The GMC mail account will be accessible by all personnel assigned to the GMC irrespective of the location they work at; GMC-Pentagon, GMC-Site R, or GMC-OSF. In the event the Pentagon is down, an alternate e-mail account will exist called "GMCBACKUP" located off of the ANMCC site.

In addition to e-mail the GMC can be reached via teleconferencing using the GCCS NewsGroups

application. The GMC-Pentagon will chair the GCCS.GMC.HELP NewsGroup discussed earlier during priority mode operations.

The GMC can be contacted via an AUTODIN message. This method should only be used if no other alternative exists. It will not be used for time-sensitive information. AUTODIN traffic should contain the following addresses. The GMC-Pentagon will be the TO addressee with the other GMC locations being INFO addressees. The addresses are:

TO: DISA Washington DC//WEY/GMC-Pentagon//
INFO: DISA Washington DC//D2/D23/D6/JEX/JEXF-OSF/JEXI//

4.7.10 Assistance from the GMC

The GMC can be contacted by GCCS sites/users whenever assistance or information concerning the GCCS is needed and cannot be obtained locally. During periods of emergency, GMC technicians may not be available to assist sites due to critical workloads. Requests should be made via the site's GCCS Site Coordinator (GSC) or Assistant GCCS Site Coordinator (AGSC). GMC technicians will work closely with the sites to identify and isolate ADP and communications related problems. When GMC personnel cannot resolve the problem, further analytical support will be obtained. The GMC will work with the GCCS site experiencing the problem to gather adequate documentation describing the problem to forward to the DISA GCCS Engineering Office.

4.7.11 GMC to DII/DISN GCC/RCCs Interface

GCCS sites/personnel requiring SIPRNET WAN or dedicated circuit assistance should contact the GMC via their GSC or AGSC. The GMC will coordinate with and refer all suspected SIPRNET WAN and dedicated circuit problems to the DII/DISN RCCs for resolution. The GMC will coordinate all communication and network outages to resolve the problem as quickly as possible and to keep each organization informed of the latest status.

4.7.12 GMC to S/A and CINC WAN Management Centers Interface

GCCS sites/personnel requiring S/A or CINC WAN or dedicated circuit assistance should contact the GMC via their GSC or AGSC. The GMC will coordinate with and refer all suspected S/A and CINC WAN and dedicated circuit problems to the S/A or CINC WAN management center for resolution. The GMC will coordinate all communication and network outages to resolve the problem as quickly as possible and to keep each organization informed of the latest status.

4.7.13 General Reporting Procedures

This section defines the recurring reporting requirements of the GCCS sites to the Joint Staff. The GMC will be responsible for receiving, compiling, and forwarding the reports to designated Joint Staff elements. The format and information required in each report is discussed below. These

reporting instructions will take effect on a date to be determined by the GCCS DIR to be announced later. Section 4.6.9 provided information on how to contact the GMC.

4.7.13.1 Scheduled Outages

Sites must notify the GMC of all scheduled outages at least 48 hours in advance. Outages under 6 hours can be approved by GMC personnel. For 6-12 hour outages, the GCCS DIR will be notified. For outages over 12 hours both the GCCS DIR and the DICO will be notified. Once an outage has been approved the GMC will enter the data into the trouble ticketing system as a planned outage where it can be tracked in the database. Planned outages scheduled less than 48 hours in advance should be reported to the GMC-HelpDesk by telephone or e-mail. For statistical purposes these short notice outages may be considered unscheduled outages. GCCS Site Coordinators should provide the following information when requesting an outage:

- GCCS site name
- Start date and time of the outage in zulu time
- Stop date and time of the outage in zulu time (or best estimate)
- Brief explanation of the outage
- Point of contact (name and telephone number)

Regularly scheduled outages such as backups, training, and preventive maintenance can be sent on a monthly basis, but no more than 30 days in advance. Specific dates, times, and explanations must be provided for each event.

4.7.13.2 Unscheduled Outages

GCCS sites will be required by Joint Pub 6-03.14 (update pending) to report GCCS outages and problems to the GMC. GCCS outages are considered the loss of hardware, software, or connectivity capabilities that degrade, impair, or severe a site's ability to perform its C2 mission. The sites must attempt to notify the GMC of all unscheduled outages within 10 minutes of the problem occurring. If the site was not manned at the time of the outage occurring then the GMC should be immediately notified on discovery of an outage. In many cases the system and network management tools will alert the GMC of major problems through the smart agents. These problems will be captured in Accugraph when the icons change color based on inputs from the SNMP manager which is fed from the smart agents. If the GMC has not heard anything from the site when a major problem occurs, they will start calling the site after 10 minutes. Status information must be reported to the GMC as it changes until the problem is resolved. The GCCS Site Coordinators should provide the following information via secure e-mail or STU-III when reporting an outage:

- Reason for Outage (RFO). Explanation of the problem
- Status of Actions. Explain what actions are being taken to resolve the problem
- Estimated Time for Repair (ETR). Best estimate of how long to fix the problem
- Corrective Action. Final closeout status report with corrective actions and restoral time

4.7.13.3 Software Cutover Report

This report will be used by the GCCS sites to report the installation of software releases or segment upgrades to the GMC. The GMC will notify GCCS Site Coordinators (GSCs) when updated versions of software are available for the suite of GCCS software. The GMC will give instructions for downloading, installation, and verification testing of the new software. A time table will be given specifying when all actions should be completed. This cutover report will provide the necessary feedback to the GMC to ensure sites have complied with said instructions. The following information will be provided via telephone or e-mail to the GMC when reporting an update to a site's software configuration:

- Software installed. Identify the individual segments and version numbers
- Time installed. Date and zulu time the software was installed in the operational system
- Problems with installation. Identify any problems encountered with installing the change

4.7.13.4 Attainment of Priority Mode Operations

Joint Pub 6-03.14 (update pending) will task the GMC with ensuring that all GCCS sites are notified and proper system and network procedures are implemented when the GCCS is placed in Priority Mode. This report will be used by the GCCS sites to notify the GMC that their facility has attained the specified priority in compliance with the procedures specified in Joint Pub 6-03.14. The GMC will be notified via telephone or e-mail for this report. If the notification is via telephone the site's GSC must follow up with an e-mail within 24 hours. If communications are down the GMC will be notified within 4 hours of the time e-mail connectivity is restored. The GCCS.GMC.HELP NewsGroup will not be used unless specifically requested. The following information will be provided to the GMC when reporting compliance with priority mode operations:

- Date and Time of Attainment. Provide date and zulu time of when the GCCS site has attained the proper mode IAW Joint Pub 6-03.14 (update pending)
- Degrade Operations. List any site GCCS system or network problems which exist at the time of the attainment. Degraded conditions as defined in Joint Pub 6-03.14 must be reported to the GMC in this subparagraph
- Special Telephone Numbers. DSN/AUTOVON telephone numbers for the GSC if the site wishes the GMC to call a special number instead of the normally used telephone number at the site

4.8 GCCS Sites

The GCCS Sites are responsible for the day-to-day operation of their local area network, applications servers, terminals, and other equipment local to the site. The GCCS sites are not responsible for the WAN equipment supplied for their site unless an Memorandum of Agreement (MOA) has been

worked out with the WAN provider. Each GCCS site must provide the support personnel for GCCS operations. Each GCCS site is categorized as either a principal GCCS Site or a secondary GCCS Site. Depending on its category, the site will have specific manning and management responsibilities. In addition, the category will determine the level of additional support that may be provided by the GMC.

4.8.1 Principal GCCS Sites

Principal GCCS sites are those directly supporting a Unified or Specified Command, the Joint Staff, or the NCAs. Most principal GCCS sites are located at command headquarters. The principal GCCS sites identified in the JCS//J-3/J-6// message DTG 0901230Z Dec 94, Subject: Global Command and Control Update, are shown in Table 9.

Acronym:	Command, Location, State or Country
ACC	Air Combat Command, Langley AFB, Hampton, VA
ACOM	Atlantic Command, Norfolk, VA
AFMC	Air Force Materiel Command, Wright-Paterson AFB, OH
AMC	Air Mobility Command, Scott AFB, IL
ANMCC	Alternate National Military Command Center, Site R
ARCENT	Army Central Command, Ft McPherson, GA
AREUR	Army European Command, Heidelburg, Germany
ARPAC	Army Pacific Command, Ft Shafter, HI
CENTAF	Central Command, Air Force, Shaw AFB, SC
CENTCOM	Central Command, MacDill AFB, Tampa, FL
CINCLANTFLT	Commander-in-Chief Atlantic Fleet, Norfolk, VA
CNO	Chief of Naval Operations, Pentagon, Washington DC
EUCOM	European Command, Stuttgart, Germany
FORSCOM	Force Command, Ft McPherson, GA
HQAF	Headquarters of the Air Force, Pentagon, Washington DC
HQDA	Headquarters, Department of the Army, Pentagon, Washington DC
HQMC	Headquarters, Marine Corps, Navy Annex, Arlington, VA
JTO	Joint Training Organization, Scott AFB, IL
MARFORLANT	Marine Forces Atlantic, Camp Lejeune, NC
MARFORPAC	Marine Forces Pacific, Camp Smith, HI
MSC	Military Sealift Command, Navy Yard, Washington DC
MTMC	Military Traffic Management Command, Army, Washington DC
NAVCENT	Navy Central Command (Rear), MacDill AFB, Tampa, FL
NAVEUR	Navy European Command, London, United Kingdom
NMCC	National Military Command Center, Pentagon, Washington DC
PACAF	Pacific Air Force, Hickam AFB, HI
PACFLT	Pacific Fleet, Makalapa, HI
PACOM	Pacific Command, Camp Smith, HI
SOCOM	Special Operations Command, MacDill AFB, Tampa, FL
SOCPAC	Special Operations Command, Pacific, Camp Smith, HI
SOUTHCOM	Southern Command, Quarry Heights, Panama
SPACECOM	Space Command, Peterson AFB, CO
STRATCOM	Strategic Command, Offutt AFB, NE
TRANSCOM	Transportation Command, Scott AFB, IL
USAFE	United States Air Force, Europe, Ramstein AB, Germany
USASOC	United States Army Special Operations Command, Ft Bragg, NC
USFK	United States Forces, Korea, Yongsan Garrison, Republic of Korea
USFK2	United States Forces, Korea 2, Taegu, Republic of Korea

Table 9 Principal GCCS Replacement Locations

An assumption is made that the principal GCCS sites have sufficient personnel with technical knowledge and expertise to manage the entire local GCCS operation.

4.8.1.1 Principal GCCS Site Manning Requirements

Principal GCCS sites are responsible for providing personnel for various roles. It is vital to understand that a single position can perform multiple roles. Additionally, some of the roles may require multiple personnel to support the size and scope of the GCCS site. Manpower requirements are being determined. The minimal roles required at a principal GCCS site are listed below. The roles were defined is section 3.4.8.3.

- GCCS Site Coordinator (GSC)
- GCCS Network Administrator (GNA)
- GCCS System Administrator (GSA)
- GCCS Database Administrator (GDBA)
- Site GCCS Designated Approving Authority (Site GCCS DAA)
- Site GCCS Information System Security Officer (Site GCCS ISSO)

4.8.1.2 Principal Site Operational Requirements

Principal sites are expected to be manned and operated 24 hours a day, 7 days a week. In instances where the site is operating under a "lights-out" concept, the site will maintain the GCCS support personnel on-call for any emergency.

The principal sites are responsible for the following as a minimum:

- LAN Management
- Data and Application Server Administration
- GCCS Site Hardware and Software Installation
- User Assistance
- Local Circuits
- Identification of Local Functional Needs.
- GCCS Site Physical and System Security

Principal sites will be subordinated to the GCCS DIR during Priority Mode operations.

4.8.1.3 GMC Support for Principal Sites

Except under Priority-Mode Operations, the GMC will limit itself to advising the principal GCCS sites on GCCS system and network issues. If requested by the site, the GMC will assist in troubleshooting the local GCCS site. During the initial fielding of the GCCS the GMC will take a more active role. Many of the GCCS sites may not have adequate system and network management software to support themselves. Once the sites (Secondary LCCs) have installed system and network

management capabilities based on direction from their S/A GCCS PMO, the GMC will take a more passive role. The support given by the GMC may be complicated by site unique equipment or configurations that are different from the DISA fielded GCCS capabilities.

4.8.2 Secondary GCCS Sites

Secondary GCCS sites are those sites indirectly supporting a Unified or Specified command without the personnel or the technical expertise to manage the entire local GCCS operation. This includes those remote sites who may only have one or two users.

4.8.2.1 Secondary GCCS Site Manning Requirements

Secondary GCCS sites are responsible for providing personnel for the following roles:

- GCCS Site Coordinator (GSC)
- Site GCCS Information System Security Officer (Site GCCS ISSO)

4.8.2.2 Secondary GCCS Site Operational Requirements

Secondary Sites are not expected to be manned and operational 24 hours a day, 7 days a week. However, the GCCS Site Coordinator is expected to be available, on-call, to assist in any eventuality.

Secondary Sites are responsible for the following as a minimum:

- Identification of Local Functional Needs.
- GCCS Site Physical and System Security

Secondary sites will be subordinated to the GCCS DIR during Priority Mode operations. During normal operations the Secondary sites are subordinated to their assigned S/A or CINC location.

4.8.2.3 GMC Support for Secondary Sites

In all likelihood the Secondary GCCS sites will not have the technical skills to manage and administer their GCCS system and network and associated equipment. It is recommended that the secondary site get help from its parent GCCS site. If that is unsuccessful then the GMC-Pentagon can be contacted to provide support. In either case, as a minimum, the following functions will be performed by either the assisting parent GCCS site or the GMC-Pentagon.

- LAN Management
- File Servers and Applications Servers Administration
- Coordination of GCCS Site Hardware and Software Installation

- User Assistance
- Assistance in Troubleshooting Local circuits

4.9 JOPES Management

The DISA/WESTHEM/JSSC, is responsible for all JOPES applications operating within today's WWMCCS. A majority of the functionality of the JOPES applications has migrated to the GCCS. The system management of the JOPES applications will be required in the GCCS environment, but several short and long term changes will occur. Those offices within JSSC supporting the WWMCCS is referred to as the GMC-JOPES for the GCCS environment. In essence they are performing the technical database management aspects of the GCCS. The functional database management is still controlled by the Joint Staff/J-33 office across the GCCS. It is imperative that the J-33 functional database personnel work in close coordination with the GMC-JOPES and vice-versa.

The major short term change is the FDBM and TDBM functions must coordinate all database activities with the GMC-Pentagon. The GCCS architecture uses primarily an Oracle database in support of various GCCS applications which include the JOPES applications. Any activities that may adversely affect the GCCS Sun Sparc 1000s and 2000s data servers must be coordinated with the GMC-Pentagon. The interaction of the software and hardware in the client-server environment is much more complex than that of the WWMCCS mainframe world. A portion of system management tools used by the WWMCCS support personnel are transitioning to the GCCS environment. While the look and feel of the JOPES system management programs may be different, GCCS support personnel will still be able to perform their mission. They will perform this mission using the GOTS GCCS System Services application.

Major long term changes will include the elimination of the JOPES unique system management software from the GCCS. The COTS products being used for system and network management of the GCCS are capable of replacing the functions of the proprietary system management software currently used by the WWMCCS FDBMs and TDBMs. In order for this change to occur, future releases of the GCCS version of the JOPES applications must include application program interfaces (APIs) for the COTS management software. Once the APIs are embedded in the GCCS version of the JOPES applications, the COTS management software can replace the proprietary management applications. Elimination of the GOTS management software will reduce the number of management applications a GMC technician must learn.

The hardware and software architecture used for the C2 mission in the GCCS changed how the applications behave. First, the average circuit data rate interconnecting GCCS sites is 10 to 30 times faster then that of the WWMCCS world. Second, the servers used in the GCCS are 100 times more powerful and faster than the WWMCCS mainframes. Third, the applications have been changed to distribute transactions differently. Instead of daisy-chaining sites together like Figure 8, the GCCS JOPES applications use a broadcast type feature to transmit data. All three of these technological improvements will lead to a faster, more responsive C2 system. Figure 24 shows the broadcast nature of how a transaction from the GCCS ACC site would travel to the other sites whose data server

contains a JOPES database.

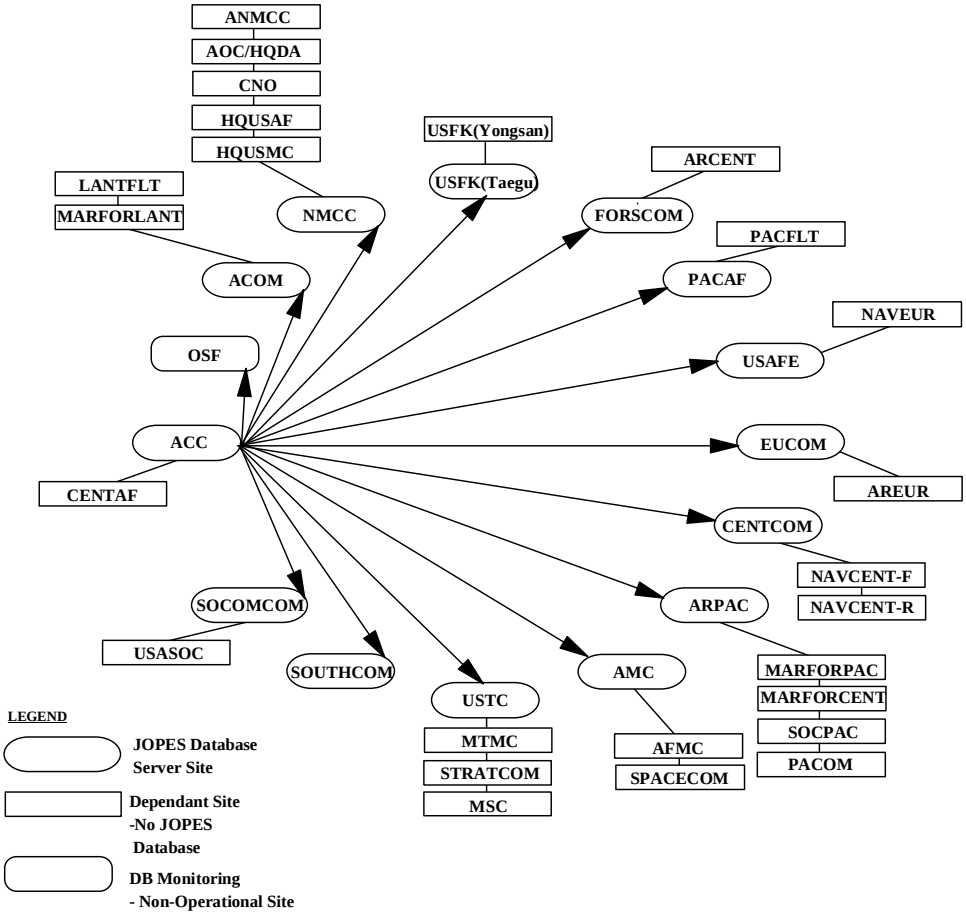


Figure 24 Example of a GCCS JOPES Transaction Broadcast

4.10 GSORTS Management

The GCCS Applications Branch (SORTS), Force Assessment Section is a subcomponent of the GMC operated by DISA/WESTHEM/JSSC. It provides force planning application support in GCCS to include operational support to users of GSORTS ADP applications and databases. Operational duties include, but are not limited to, the following:

- Update the GSORTS databases at all approved sites twice daily (daily on holidays and weekends)
- Monitor and maintain the GSORTS teleconference (GCCS.GSORTS.NEWS)
- Monitor GSORTS reporting transactions
- Perform quality assurance checks on the master GSORTS database

- Test/validate problem resolutions and new code
- Support data entry tools
- Provide backups/saves of the joint database and reference files
- Register DOD, Joint Staff, and defense agencies
- Maintain SORTS tables in the joint database
- Provide recurring data retrieval support
- Provide user training
- Maintain standard operating procedural document

The Force Assessment Section coordinates all database activities with the GMC-HelpDesk. This is because any activities that may adversely affect the GCCS Sun Sparc 1000s and 2000s data servers must be coordinated. The COTS products being used for system and network management of the GCCS will be tested to see how they can improve the performance monitoring capabilities of GSORTS. This may require future releases of the GSORTS application to include APIs for the COTS management software. This approach should help reduce the number of management applications a GMC technician must learn.

4.11 Exchanging of Peer-to-Peer Management Data

System and network management data can be exchanged on a peer-to-peer basis between intelligent managers or expert engines within an integrated enterprise management system. Also, system and network management data can be gathered by continually polling elements across the network. The later is the least desirable method for collecting data. This is because polling can add considerable overhead on a LAN or WAN taking away available bandwidth that could be used by operational data. The GCCS will rely heavily on outside organizations within DISA for data transport via the SIPRNET routers, the SIPRNET communications servers, or the ITSDN routers. Additionally, the GCCS will use S/A and CINC networks to provide WAN connectivity for many of the smaller, geographically separated GCCS sites. Internal management of the GCCS will be a collective effort between the GMC sites (Primary LCCs) and the system and network management capabilities of the GCCS sites (Secondary LCCs). Not all of the GCCS sites will have system and network management capabilities. Several of the S/As are implementing base or service wide NMCs for controlling all of their networks. This mixture of service approaches to system and network management will complicate GCCS site (Secondary LCCs) management responsibilities.

Figure 25 attempts to show the interaction between various organizations with system or network management and the GMC for the GCCS. The GMC is the focal point for all GCCS system and network management activities. It is crucial to the GMC to receive input from those organizations providing WAN services, the DISN/DII RCCs, and the S/A and CINC WAN management centers. Interaction with these organizations will allow the GMC to see the health of the other DoD transport systems it relies on. In turn, if requested, the GMC can provide management data to these organizations. Interaction with the individual GCCS sites becomes more complicated. Interaction with the sites may be from a site's system and network management function (Secondary LCCs) or from an S/A Management Center responsible for the particular GCCS site. In all cases, a

bidirectional exchange of management data is possible as the figure indicated.

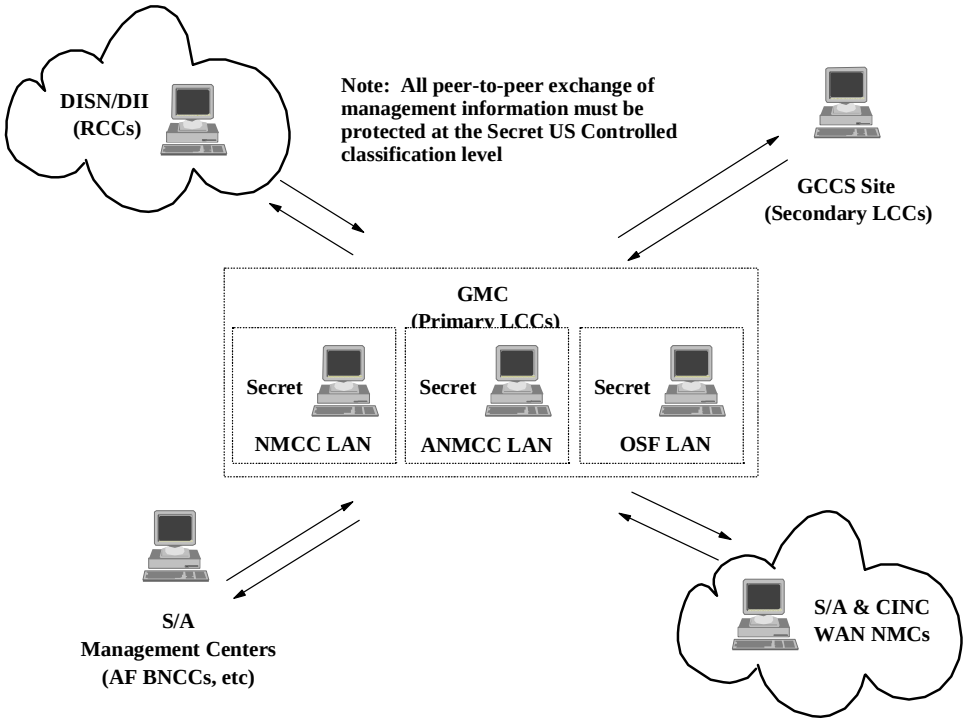


Figure 25 Peer-to-peer Exchanging of Management Data

CINCs want to see the health and status of their subordinate sites. This can be achieved in two ways. First, the future implementation plans for the GMC architecture calls for Accugraph and Remedy to be made available to the site's GSC, GNA, GSA, GDBA, and Site GCCS ISSO personnel. However, this will take some time to get implemented and does not satisfy the CINCs and S/As immediate concerns of being able to see their sites. The second way involves the smart agents installed at the GCCS sites. They are one of the major sources of information for the GMC. These agents gather fault and performance data and send this information back via SNMP and SMTP to the GMC-Pentagon and GMC-OSF as explained in the earlier sections. This is how DISA satisfies its role to the Joint Staff of providing oversight management of the GCCS. These agents are programed with the IP address or DNS name of the SNMP management workstation they report data to. They can report to more than one workstation. It is mandatory to have the two GMC locations programmed in the agent but additional management platforms can be added. Through this mailing list mechanism additional locations wanting to receive the management data can do so. It is strongly encouraged the local site receive the management data. If a CINC or S/A wants to see this data they only have to be added to the mailing list of the sites they want to see. All management platforms would receive the data equally in near real time.

Figure 26 shows the example of a site's smart agents and how they can report to multiple locations.

This figure is based on Figures 21 and 25 and shows how the two can be combined. The figure does not represent all the locations the data could go to, other may exist. The figure does show though how the CINCs and S/As can have a view now into their GCCS sites.

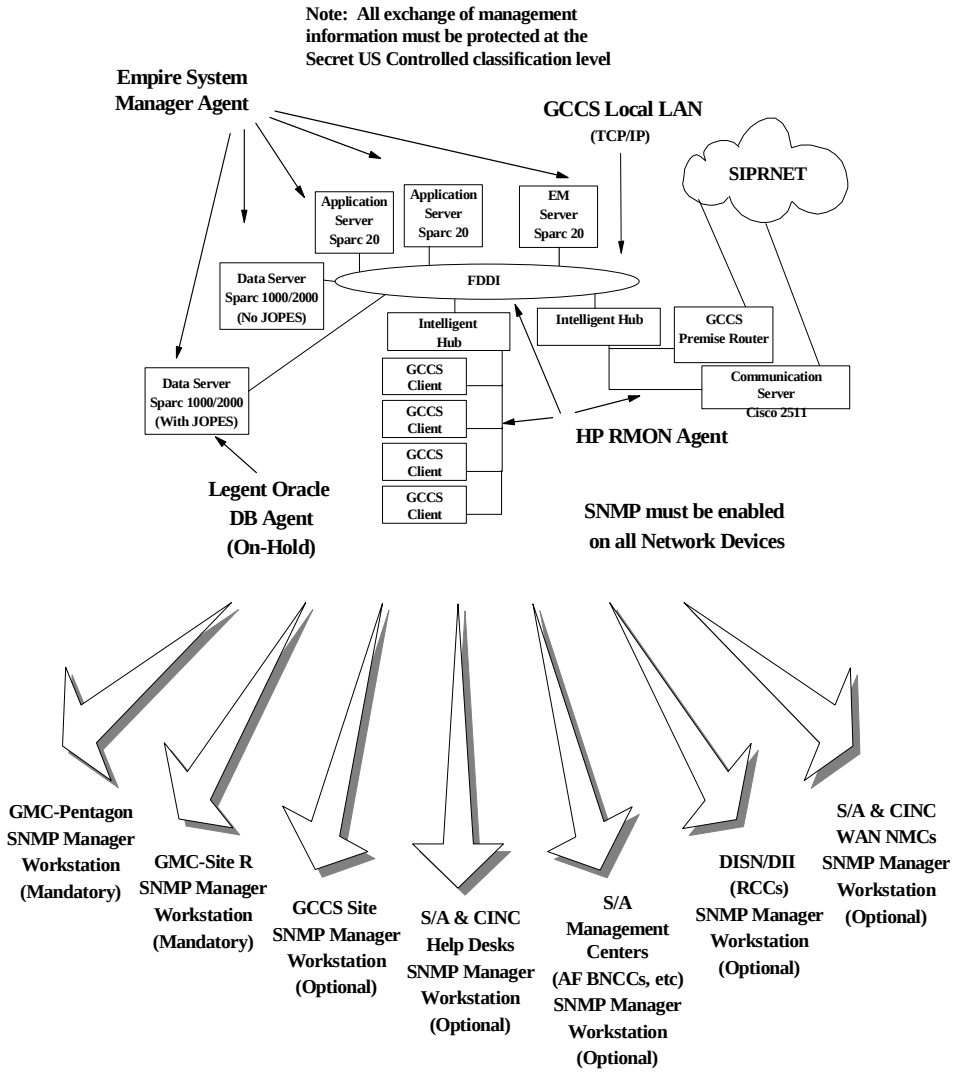


Figure 26 Multiple Reporting From Smart Agents

One final concern is the classification of management data being exchanged. Some of the data that may be reported from the GMC or Secondary LCCs at the sites or S/A NMCs will be classified. Events trapped and reported via the management data that reveal vulnerabilities or significant loss of warfighting capabilities within the GCCS will be classified. All management centers receiving this classified management data must take the necessary safeguards of protection.

The following sections will identify the types of management data to be exchanged automatically between various management centers. Most of the data identified pertains to fault and performance management. As security management is integrated more thoroughly with the operations of the DII GCC and RCCs, this type of data will also be exchanged. The types of data to be exchanged listed below is not all inclusive nor permanent in nature. Also, as standards are developed within the DoD for exchanging management data the format for the data may change. Additionally, as the GCCS matures, additions and deletions to the type data being exchanged will occur. The decision authority for authorizing these changes for the GCCS management structure is the GCCS DIR.

4.11.1 GMC to DISN/DII

The GMC will provide the following fault management data to the RCCs of the DISN/DII.

- Failure of a GCCS premise router
- Restoral of a GCCS premise router
- Total failure of a GCCS site's communications server capabilities
- Restoral of a GCCS site's communications server capabilities

4.11.2 DISN/DII to GMC

The DISN/DII RCCs will provide the following fault management data to the GMC.

- Failure of a SIPRNET WAN router
- Restoral of a SIPRNET WAN router
- Failure of a SIPRNET intra-router trunk (IRT)
- Restoral of a SIPRNET intra-router trunk (IRT)
- Failure of an ITSDN router
- Restoral of an ITSDN router
- Failure of an ITSDN to SIPRNET access circuit
- Restoral of an ITSDN to SIPRNET access circuit
- Failure of a SIPRNET communications server
- Restoral of a SIPRNET communications server

The DISN/DII will provide the following performance management data to the GMC on a bi-monthly interval. Ad hoc reports will be generated on an out of cycle basis when required for operational needs on a fee for service basis.

- Overall utilization of the SIPRNET WAN
- Statistics on IRT utilization within the SIPRNET WAN
- Statistics on access circuit utilization between SIPRNET and GCCS premise routers
- Statistics on access circuit utilization between SIPRNET and S/A WAN routers supporting the GCCS

4.11.3 GMC to S/As Management Centers

The GMC will provide the following fault management data to the management centers operated by the S/As either service wide or base wide.

- Failure of a GCCS premise router
- Restoral of a GCCS premise router
- Total failure of a GCCS site's communications server capabilities
- Restoral of a GCCS site's communications server capabilities
- Total failure of a GCCS site
- Restoral of a GCCS site

4.11.4 S/As Management Centers to GMC

The S/As management centers will provide the following fault management data to the GMC.

- Failure of an S/A router supporting GCCS data traffic
- Restoral of an S/A router supporting GCCS data traffic
- Failure of an S/A intra-router trunk (IRT)
- Restoral of an S/A intra-router trunk (IRT)
- Failure of an S/A WAN to SIPRNET WAN access circuit
- Restoral of an S/A WAN to SIPRNET WAN access circuit
- Failure of an S/A communications server supporting GCCS data traffic
- Restoral of an S/A communications server supporting GCCS data traffic

4.11.5 GMC to GCCS Site

The GMC will provide the following fault management data on request to the GCCS sites operating an enterprise management system.

- Failure of a GCCS premise router
- Restoral of a GCCS premise router
- Total failure of a GCCS site's communications server capabilities
- Restoral of a GCCS site's communications server capabilities

4.11.6 GCCS Site to GMC

The GCCS sites will provide the following fault management data to the GMC.

- Failure of a site secondary router supporting a campus environment
- Restoral of a site secondary router supporting a campus environment
- Failure of a site campus router trunk
- Restoral of a site campus router trunk

4.11.7 GMC to S/A WAN

The GMC will provide the following fault management data to the NMC of the S/A WAN if requested:

- Failure of a GCCS premise router
- Restoral of a GCCS premise router
- Total failure of a GCCS site's communications server capabilities
- Restoral of a GCCS site's communications server capabilities

4.11.8 S/A WAN to GMC

The S/A WAN NMC will provide the following fault management data to the GMC.

- Failure of a S/A WAN router
- Restoral of a S/A WAN router
- Failure of a S/A intra-router trunk (IRT)
- Restoral of a S/A intra-router trunk (IRT)

The S/A NMCs will provide the following performance management data to the GMC on a weekly and monthly interval.

- Overall utilization of the S/A WAN
- Statistics on IRT utilization within the S/A WAN
- Statistics on access circuit utilization between the S/A WAN and GCCS premise routers
- Statistics on access circuit utilization between SIPRNET and S/A WAN routers

4.11.9 Additional Peer Management Requirements

A large number of secondary GCCS sites will be connected to the GCCS via the SIPRNET by traversing through CINC or S/A WANs or multiplexer networks. An example of this would be the Air Force Command and Control Network (AFC2N) which is a WAN network supporting Air Force secondary GCCS sites. To ensure these networks are robust enough to support GCCS operations, monthly performance reports will be required.

The S/A or CINC PMOs responsible for the WANs will make available to the GCCS DIR monthly reports concerning the operational status of any S/A or CINC WAN or communications network supporting GCCS sites. These reports will include, but are not limited to, network traffic loads, throughput, equipment outages, circuit utilization rates, packet drop rates, and throughput delay rates. All reports will be used as the basis for determining if S/A or CINC WANs or communications networks are operating within acceptable limits for the GCCS mission. The reports will be used as a determining factor for recommending improvement to CINC or S/A communications assets. When practical, these reports may be posted to a web site so CINCs, S/As, and GCCS sites can have access to the data. Specific details, including security concerns, will be worked out during implementation.

4.12 Access and Permissions

The success or failure of system and network management depends heavily on the ability to install monitoring software (smart agents) on the GCCS hardware platforms and then to access the software using the various management protocols. To this end management protocols must be able to flow freely throughout the GCCS and supporting infrastructures. This includes the SIPRNET and S/A and CINC WANs. No network, firewall, or security implementation will block SNMPv1, SNMPv2, CMIP, or OMNIPoint protocol operating between the various GMC locations and GCCS sites of any size or scope. The Joint Staff/J-61 formal message, DTG 131731Z DEC 95, Subj: Activation of Simple Network Management Protocol (SNMP) for Global Command and Control System (GCCS), directed the implementation of these actions for the GCCS sites and all support WAN networks. This policy will provide the necessary access to the GCCS sites.

One of two alternatives is required to ensure quick reallocation of resources in the event the Joint Staff/J-3 has placed portions of the GCCS into Priority Mode to support a national crisis or contingency. The GMC locations also will require read/write access to all GCCS premise routers, GCCS communications servers, and other network devices supporting the GCCS owned and operated at the GCCS sites. If the GCCS user considers provision of write access to the GMCs as an unacceptable security risk, or for other reasons does not wish to provide that access, the GCCS sites will allocate their manning to provide the ability to make directed changes to the routers, communications servers, and network devices within and not later than 60 minutes following issuance of direction from the Joint Staff/J-3. In all cases, any changes will be coordinated with the GCCS Site Coordinator when time permits.

The GMC locations will require read-only access to all news, HTTP, mail, database, application, EM, primary NFS mount points, OPS/INTEL, and MAP servers at GCCS locations with 24 hour on-site maintenance. For those locations without 24 hour coverage, the GMC locations will require read/write access to the servers unless the site can react within and not later than 60 minutes following issuance of directed changes from the Joint Staff/J-3. This does not conflict with the site's responsibility for day-to-day maintenance. Without this access, the GMC can not assist in troubleshooting or perform the joint oversight mission during Priority Mode operations. In all cases,

any actions will be coordinated with the GCCS Site Coordinator, the GCCS System Administrator,

and the site's GCCS Database Administrator if time permits.

GMC personnel will require access to the joint hardware and software operating at the GCCS sites. Under the current security architecture this will require these individuals to have accounts on the Executive Manager (EM) server at each location. Future releases of the EM server software, in conjunction with security policies, may support a watchdesk type account. For now, a one-to-one accountability must exist within the GCCS.

In those cases where the GMC must have read/write access to a site's capability, only a small cadre of personnel at the GMC will be given the access. These individuals will be both functional and technical experts who are officially designated to have access to specific sites. Every such person will be designated in writing and approved by the GCCS ISSO for the GMC and approved by the site's GCCS ISSO for which they have access. All persons will comply with the CM and security accreditation requirements for the site.

By implementing the above access and permissions guidelines the GMC can perform its global mission. GCCS sites must take no actions that will blind the GMC infrastructure, thus defeating the global management concept.

GLOSSARY

ACC	Air Combat Command
ACL	Access Control List
ACOM	Atlantic Command
ADP	Automatic Data Processing
ADNET	AntiDrug Network
AETC	Air Education and Training Command
AFMC	Air Force Materiel Command
AGSC	Assistant GCCS Site Coordinator
AHIP	ARPANET - Host Interface Protocol
AIG	Address Indicator Group
AIS	Automated Information System
AM	Accounting Management
AMC	Air Mobility Command
AMHS	Automated Message Handling System
ANMCC	Alternate National Military Command Center
API	Application Program Interface
ARCENT	Army Central Command
ARPAC	Army Pacific Command
AUTODIN	Automatic Digital Network
AUTOVON	Automatic Voice Network (now DSN)
AWC	US Army War College
BBN	Bolt, Baranek, and Newman, Inc.
BGP	Border Gateway Protocol
BNCC	Base-level Network Control Center
BPS	bits per second
C2	Command and Control
C3	Command, Control, and Communications
C3I	Command, Control, Communications and Intelligence
C4I	Command, Control, Communications, Computers and Intelligence
C4IFTW	C4I for the Warrior
CCB	Configuration Control Board
CCITT	International Telegraph and Telephone Consultative Committee
CE	Communications Element
CENTAF	Central Command, Air Force
CENTCOM	Central Command
CIK	Crypto Ignition Key
CINC	Commander in Chief of a Unified Command
CINCLANTFLT	Commander in Chief Atlantic Fleet
CJCS	Chairman, Joint Chiefs of Staff

CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJTF	Commander, Joint Task Force
C/JTF	Combined/Joint Task Force
CM	Configuration Management
CMC	Commandant, US Marine Corps
CMIP	Common Management Information Protocol
CMW	Compartmented Mode Workstation
CNO	Chief of Naval Operations
COE	Common Operating Environment
CONOPS	Concept of Operations
CONUS	Continental United States
COTS	Commercial Off-The-Shelf
CPPP	Compressed Point-to-Point Protocol
CS	Communications Server
C/S	Client/Server
CSLIP	Compressed Serial Line Interface Protocol
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DB	Database
DBA	Database Administrator
DBM	Database Manager
DCA	Defense Communications Agency (now DISA)
DCA NMOC	DCA Network Management Operations Center (first renamed to DISA NMOC but is now called the DII GCC)
DCE	Distributed Computing Environment
DCS	Defense Communications System
DCS-EP	Defense Communications System - Entry Point
DDN	Defense Data Network
DGSA	DoD Goal Security Architecture
DIA	Defense Intelligence Agency
DICO	Data Information Coordination Officer
DII	Defense Information Infrastructure
DIICC	Defense Information Infrastructure Control Concept
DIR	Director
DISA	Defense Information Systems Agency
DISA NMOC	DISA Network Management Operations Center (now called the DII GCC, formerly the DCA NMOC)
DISN	Defense Information System Network
DISN-EP	Defense Information System Network - Entry Point
DMA	Defense Mapping Agency
DMC	Defense Megacenter
DMS	Defense Message System

DNS	Domain Name Service
DoD	Department of Defense
DoDIIS	DoD Intelligence Information System
DSCS	Defense Satellite Communications System
DSN	Defense Switched Network (formerly AUTOVON)
DSNET1	Defense Secure Network One
DSNET2	Defense Secure Network Two
DSNET3	Defense Secure Network Three
DSS	Digital Signature Standard
DSSO	Defense Systems Support Organization
DTG	Date Time Group
ECP	Engineering Change Proposal
E^3	End-to-End Encryption
ETR	Estimated Time for Repair
EUCOM	European Command
FDBM	Functional Database Manager (WWMCCS)
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standard
FM	fault management
FM	Functional Manager (WWMCCS)
FMA	Functional Management Area
FOC	Final Operational Capability
FOC	Full Operational Capability
FORSCOM	Forces Command
FOUO	For Official Use Only
FTP	File Transfer Protocol
GB	Gigabytes
GCC	Global Control Center
GCCS	Global Command and Control System
GCCS DIR	Global Command and Control System Director
GCCS(T)	Global Command and Control System (Top Secret)
GDBA	GCCS Database Administrator
GFE	Government Furnished Equipment
GIS	GCCS Information System
GMC	GCCS Management Center
GCCS.GMC.HELP	GCCS Management Center Conference (NewsGroup)
GNA	GCCS Network Administrator
GNMP	Government Network Management Profile
GNOC	GCCS Network Operations Center
GOSIP	Government Open Systems Interconnection Profile

GOTS	Government Off-The-Shelf
GSA	GCCS System Administrator
GSC	GCCS Site Coordinator
GSM	GCCS Security Management
GSO	GCCS Security Officer (Joint Staff J6 designee)
GUI	Graphical User Interface
HP	Hewlett Packard
HQAF	Headquarters of the Air Force
HQDA	Headquarters, Department of the Army
HQMC	Headquarters, Marine Corps
HR	Host Resources
IAB	Internet Architecture Board
IAB STD	Internet Architecture Board Standard
IAW	In Accordance With
IDNX	Integrated Digital Network Exchange
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGOSS	Industry/Government Open Systems Specifications
ILSP	Integrated Logistic Support Plan
IOC	Initial Operational Capability
IP	Internet Protocol
IPR	Internet Protocol Router
IRT	Inter-Router Trunk
IS	Information System
ISO	International Standards Organization
ISSO	Information System Security Officer
ITSDN	Integrated Tactical Strategic Data Networking
ITU-TS	International Telecommunications Union - Technology Sector
J3	Director of Operations, Joint Staff
J6	Director for Command, Control, Communications and Computer Systems, Joint Staff
JANAP	Joint Army, Navy, Air Force Publications
JCCC	Joint Communications Control Center (JTF related)
JCPMS	Joint Communications Planning and Management System
JCS	Joint Chiefs of Staff
JDEF	Joint Demonstration and Evaluation Facility
JIEO	Joint Interoperability & Engineering Organization (formerly DSSO)
JILSP	Joint Integrated Logistics Support Plan
JITC	Joint Interoperability Test Command
JNOCC	JOPES Network Operations Control Center

JOPES	Joint Operations Planning and Execution System
JTO	Joint Training Organization
JTF	Joint Task Force
JTF Net	Joint Task Force Network
JWICS	Joint Worldwide Intelligence Communications System
kbps	kilo-bits per second
LAN	Local Area Network
LCC	Local Control Center
MAC	Mandatory Access Control
MARCORSYSCOM	Marine Corps Systems Command
MARFORLANT	Marine Forces Atlantic
MARFORPAC	Marine Forces Pacific
MIB	Management Information Base
MIB-II	Management Information Base - II
MIL-HDBK	Military Handbook
MIL-STD	Military Standard
MILNET	Military Network
MLS	Multi-Level Security
MNS	Mission Need Statement
MOA	Memorandum of Agreement
MOM	Manager-Of-Managers
MSC	major subordinate command (USMC)
MSC	Military Sealift Command
MS DOS	Microsoft Disk Operating System
MTMC	Military Traffic Management Command
NATO	North Atlantic Treaty Organization
NAVCENT	Navy Central Command
NAVEUR	Navy European Command
NCA	National Command Authorities
NCSC	National Computer Security Center
NES	Network Encryption System
NEACP	National Emergency Airborne Command Post
NIC	Network Information Center
NIPRNET	Unclassified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NLSP	Network Layer Security Protocol
NM	Network Management
NMC	Network Management Center
NMCC	National Military Command Center

NMCS	National Military Command System
NMF	Network Management Forum
NOC	Network Operations Center
NOFORN	Not-Releasable to Foreign Nationals (obsolete security term)
NSA	National Security Agency
NTIS	National Technical Information Services
NTISSI	National Telecommunications Information System Security Instruction
OASD/C3I	Office of the Assistant Secretary of Defense for C3I
OCONUS	Outside the Continental United States
OIC	Officer In Charge
OIW	Open Systems Management Implementors Workshop
OMNIPoint	Open Management Interoperability Point
OPLAN	Operation Plan
OPR	Office of Primary Responsibility
OSD	Office of the Secretary of Defense
OSF	Operational Support Facility
OSI	Open System Interconnection
PACAF	Pacific Air Force
PACFLT	Pacific Fleet
PACOM	Pacific Command
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
POC	Point-of-Contact
PM	Performance Management
PM	Preventive Maintenance
PM	Program Manager
PMO	Program Management Office
POSIT	Profiles for Open Systems Internetworking Technologies
POSIX	Portable Operating System Interface
PPP	Point-to-Point Protocol
PSN	Packet Switch Node
RAM	Random Access Memory
RCC	Regional Control Center
RDBMS	Relational Database Management System
RFC	Request for Comment
RFO	Reason for Outage
RMON MIB	Remote Monitoring Management Information Base
S/A	Service/Agency
SAT	Secure AUTODIN Terminal

SAT	Standard Automated Terminal
SATAN	Security Administrator Tool for Analyzing Networks
SCC	Security Classification Code
SCSI	Small Computer System Interface
SIPRNET	Secret Internet Protocol Router Network
SLIP	Serial Line Interface Protocol
SM	Security Management
SMC	System Management Center
SMG	Secure Mail Guard
SMIB	Security Management Information Base
SNMP	Simple Network Management Protocol
SNMPv1	Simple Network Management Protocol, Version 1
SNMPv2	Simple Network Management Protocol, Version 2
SNS	Secure Network Server
SOCOM	Special Operations Command
SOCPAC	Special Operations Command, Pacific
SOUTHCOM	Southern Command
SPACECOM	Space Command
SPIRIT	Service Provider Integrated Requirements for Information Technology
SQL	Structured Query Language
SSC	SIPRNET Support Center
STRATCOM	Strategic Command
STU-III	Secure Telephone Unit - III
TAFIM	Technical Architecture for Information Management
TBD	To Be Determined
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDB	Transaction Database
TDBM	Technical Database Manager
TDY	Temporary Duty
TFM	Trusted Facility Manual
TIP	Technology Insertion Project
TLCF	Teleconferencing Program
TPFDD	Time-Phased Force Deployment Data
TRANSCOM	Transportation Command
TS	Top Secret
TS3	Top Secret Support System
USAFE	United States Air Force, Europe
USASOC	United States Army Special Operations Command
USFJ	United States Forces, Japan

USFK	United States Forces, Korea
USFK2	United States Forces, Korea 2 (alternate site)
VAS	Value Added Service
WAN	Wide Area Network
WASO	WWMCCS ADP Security Officer
WASSO	WWMCCS ADP System Security Officer (site)
WIN	WWMCCS Information Network
WIS	WWMCCS Information System
WS	Workstation
WSC	WIN Site Coordinator
WWMCCS	Worldwide Military Command and Control System
WWS	WWMCCS Workstation

REFERENCES

This section contains reference materials that will expand the reader's understanding of system and network management concepts, existing WWMCCS operations and concepts, planned GCCS operations and concepts, and other miscellaneous documents. Most of the public domain documentation can be obtained in electronic soft copy via anonymous ftp retrieval. When using anonymous ftp, login to the remote host as *anonymous* and use the password *anonymous*, *guest*, or your e-mail address. Specific password instructions usually are given during the login process. When possible, the remote host and path/filename are given for the documents listed below.

R.1 Government Documents

R.1.1 General DoD and Federal Documents

The following specifications, standards, and handbooks are used to varying degrees to build the foundation of this document. Unless otherwise specified, the issues of these documents are those listed in the Department of Defense Index of Specifications and Standards (DoDISS) and supplements. Copies of these documents can be obtained from:

Documents Order Desk
Building 4D
700 Robbins Avenue
Philadelphia, PA 19111-5094

Copies of Federal Information Processing Standards (FIPS) and those documents published by the National Institute of Standards and Technology (NIST) may be obtained from:

National Technical Information Services (NTIS)
U.S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161

or:

Standards Office, NIST
Building 225, Room B64
Gaithersburg, MD 20899
(301) - 975-2816

Documents:

(1) Department of Defense, DoD Directive 5200.28, *Security Requirements for Automated Information Systems (AISs)*, 21 March 1988.

(2) Department of Defense, DoD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985 (Orange Book).

(3) FIPS Publication 179, *Government Network Management Profile (GNMP)*, 15 Dec 92.
Electronic ftp retrieval
Remote host = osi.ncsl.nist.gov Path/filename = pub/gnmp

(4) FIPS Publication 146-1, *Government Open Systems Interconnection Profile (GOSIP), Version 2.0*, 3 Apr 91.
Electronic ftp retrieval
Remote host = osi.ncsl.nist.gov Path/filename = pub/gosip

(5) *Industry/Government Open Systems Specifications (IGOSS), Version 1*, May 94.
Electronic ftp retrieval
Remote host = osi.ncsl.nist.gov Path/filename = pub/igoss

(6) MIL-STD-2045-17507, *Internet Network Management Profile for DoD Communications, Parts 1-3*, DRAFT, 1 June 1994.

(7) MIL-HNBK-1351, *Network Management for DoD Communications*, 23 Jul 93.

(8) NIST Special Publication 500-214, *Stable Implementation Agreements for Open Systems Interconnection Protocols, Open Systems Environment Implementors Workshop (OIW), Version 7, Edition 1*, Dec 93.
Electronic ftp retrieval
Remote host = nemo.ncsl.nist.gov Path/filename = pub/oiw/agreements/

(9) MIL-STD-2045-38000, *Network Management of DoD Communications*, DRAFT, 4 January 1993.

(10) Military STD.401, *Secure Data Network Systems (SDNS) Security Protocol 4 (SP4), Revision 1.3*, National Security Agency.

(11) NISTIR 4792, *A Formal Description of the SDNS Security Protocol at Layer 4 (SP4)*, Wayne Janse, Mar 92.

(12) *Department of Defense Technical Architecture Framework for Information Management, Version 2.0*, March 1995. OPR: DISA.
Electronic retrieval
www = http://www.itsi.disa.mil/cfs/tafim.html

(13) MIL-STD-498, *Software Development and Documentation*, 5 December 1994.

(14) MIL-STD-973, *Configuration Management,* 17 April 1992.

(15) Department of Defense, DoD Handbook 5200-H, *Department of Defense Handbook for Writing Classification Guidance*.

(16) Department of Defense, DoD Index 5200-I, *Index of Security Classification Guides.*

(17) Department of Defense, DoD Pamphlet 5200-PH, *A Guide to Marking Classified Documents.*

(18) CJCSI 6212.01, *Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems*, 30 July 1993.

(19) Department of Defense, DoD Regulation 5200.1, *DOD Information Security Program*.

(20) Department of Defense, DoD Regulation 5200.2, *DOD Personnel Security Program*.

(21) Draft *System Engineering Guidelines for the Implementation of a Base-Level Network Control Center,* 30 December 1994. OPR: AFC4A/TNSCC, Scott AFB IL.

(22) CSC-STD-002-85, Department of Defense Password Management Guidelines, 12 April 1985.

(23) Department of Defense, DoD Directive 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*, 16 June 1992.

(24) Department of Defense, DoD Directive C-5200.5, *Communications Security (COMSEC)*, 21 April 1990.

(25) Department of Defense, DoD Directive C-5200.19, *Control of Compromising Emanations*, 23 February 1990.

(26) NTISSI No. 7000, *TEMPEST Countermeasures for Facilities*, 29 November 1993.

R.1.2 WWMCCS Specific Publications

(1) *Joint Operation Planning and Execution System (JOPES), Functional Data Base Manager (FDBM), Users Manual - Volume 4,* TD 18-14-1 Vol 4, 15 September 1994. OPR: DISA/JISC/UJNCP.

(2) *Joint Operation Planning and Execution System (JOPES), Technical Database Manager's (TDBM) Handbook*, TD 18-64, 28 June 1993. OPR: DSSO/JNCP.

(3) CSM 339-92, Volume 1, *Joint Operation Planning and Execution System (JOPES) Computer System Users Manual*. General reference includes reference information applicable to the whole system.

(4) Joint Pub 6-03.14, *Operation and Management of the WWMCCS Intercomputer Network (WIN)*. OPR: JCS/J6C.

(5) *WWMCCS Intercomputer Network (WIN), Technical Instruction (TI)*, dated 15 October 1992. OPR: JCS/J6C.

(6) DCA Circular 310-130-2, 13 February 1979, and DCA message DTG 271203Z January 1989, *Defense Communications System Management Thresholds (MT) and Performance Objectives (PO)*.

(7) DCA Circular 370-P185-15, *WWMCCS ADP Standard Telecommunications Engineering Practices*, March 1988.

(8) DCA Circular 310-P70-76, *Node Site Coordinator Guide*, Sep 1986.

(9) *Automatic Digital Network (AUTODIN) Operating Procedures*, JANAP 128.

(10) *Security Policy for the WWMCCS Intercomputer Network*, Joint Pub 6-03.7 (current edition)

(11) *Joint Operation Planning and Execution System (JOPES), Technical Database Manager's (TDBM), Handbook*, TD 18-64, 28 June 1993. OPR: DISA/JISC/UJNCP.

R.1.3 GCCS Specific Publications

This section lists documents that are specific to the GCCS program. While some are the basis for this document, others are for completeness in understanding the GCCS program. Copies of these documents can be obtained by contacting the DISA/JIEO Configuration Management Department library at commercial (703) 735-8764/8669/8668 or DSN 653-8764/8669/8668. Copies are available in either hardcopy or softcopy form.

(1) Draft *GCCS Systems Management Implementation Plan and Procedures*, 19 May 1995. OPR: DISA/JEXIT.

(2) *GCCS Common Operating Environment Requirements*, 15 August 1994. OPR: DISA/JEAC.

(3) *GCCS Baseline Common Operating Environment*, 28 November 1994. OPR: DISA/JEAC.

(4) Draft CJCSI xxxx.xx, *Global Command and Control System (GCCS), Configuration Management Policy*, 13 June 1995. OPR: JCS/J6

(5) Draft *Global Command and Control System (GCCS), Classification Guide*, 6 June 1995. OPR: DISA/JEAC.

(6) Draft *Global Command and Control System (GCCS), Joint Integrated Logistics Support Plan*, 8 June 1995. OPR: DISA/JIEO/D23.

(7) CJCSI 6721.01, *Global Command and Control Management Structure*, 18 February 1995.

(8) *Validation Approval of Mission Need Statement (MNS) for Global Command and Control System (GCCS)*, 8 June 1995. OPR: JCS/J6V.

(9) *Global Command and Control System, Concept of Operations (CONOPS)*, 11 April 1995. OPR: JCS/J36

(10) *Global Command and Control System, Migration Director Charter*, 6 January 1995. OPR: DISA/D23.

(11) *Global Command and Control System, Program Management Plan*, 29 March 1995. OPR: DISA/D23.

(12) *Global Command and Control System, Functional Economic Analysis*, 30 March 1995. OPR: DISA/D623.

(13) *Global Command and Control System, Test and Evaluation Master Plan*, 17 March 1995. OPR: DISA/JEEXC.

(14) *Global Command and Control System, Operational Evaluation Master Plan*, 7 March 1995. OPR: DISA/JEEXC.

(15) *Global Command and Control System, Training Concept*, 10 February 1995. OPR: DISA/D23.

(16) Global Command and Control System, *Joint Integrated Logistics Support Plan*, 8 June 1995. OPR: DISA/D23.

(17) Global Command and Control System, *Migration Strategy*, 22 March 1995. OPR: DISA/D23.

(18) Global Command and Control System, *JOPES Training Organization Course Catalog*. OPR: TRANSCOM. Telephone: (618)-256-8042.

(19) *Global Command and Control System Functional Requirements Evaluation Procedures,* 21 April 1995. OPR: JCS/J36CSOD.

(20) Draft *GCCS Automated Information System (AIS), Security Plan for Version 2.0*, 21 April 1995. OPR: DISA/JIEO/JEXNW.

(21) *GCCS System Security Implementation Instructions for Site Security Administrators for Version 2.0,* 12 May 1995. OPR: DISA/JIEO/JEXNW.

(22) CJCSI 6731.01, *Global Command and Control Security Policy*, December 1994.

(23) *Global Command and Control System (GCCS) Trusted Facility Manual for Version 2.0,* 12 May 1995. OPR: DISA/JIEO/JEXNW.

(24) ASD C3I Memorandum, *Selection of Migration Systems,* 12 November 1993.

(25) Draft *User's Logistics Support Summary (LSS) for the Global Command and Control System (GCCS)*, 27 February 1995.

(26) Draft *Global Command and Control System, Technical Security Functional Requirements Document,* 10 March 1995. OPR: DISA/JIEO/JEXI.

(27) Draft *Global Command and Control System (GCCS) V2.0 Security Features Users Guide*, 12 May 1995. OPR: DISA/JIEO/D23.

R.1.4 Other DISA Non-GCCS/WWMCCS Publications

(1) *Defense Information System Network, Integrated Tactical Strategic Data Networking (ITSDN), Internet Protocol Addressing Plan,* 24 June 1994. OPR: DISA/JIEO/JEEFE

(2) Draft *Defense Information System Network, Dial-In Data Services, Internet Protocol Addressing Plan*. OPR: DISA/JIEO/JEEFE

(3) *Defense Information System Network, Secret Internet Protocol Network (SIPRNET) Addressing Plan*. OPR: DISA/JIEO/JEEFE

(4) *Defense Information System Network, Secret Internet Protocol Network (SIPRNET) Router Architecture Plan*. OPR: DISA/JIEO/JEEFE

(5) DISA Circular 310-70-X, *Methods and Procedures, DII Control Centers*. OPR: DISA/D5

(6) DISA Technical Report 93-07-C, Joint Task Force Communications Planning and Management Concept of Operations, Final Report. OPR: DISA/JIEO/JEEPB

(7) CJCSM 6231 *Employment of Joint Tactical Communications Systems, Volume 7, Network Management.* OPR: Joint Staff/J-6

(8) DISA/JIEO Report 8125, *Joint Task Force Tactical Communications Architecture,* March 1995. OPR: DISA/JIEO

R.2 Non-Government Publications

The following documents are used in part as references for building this document. A thorough understanding of these documents by the reader will aid in understanding system and network management.

R.2.1 Industry Standards

Industry standards are developed by the International Standards Organization (ISO) and the International Telecommunications Union - Technology Sector (ITU-TS) formerly known as the International Telegraph and Telephone Consultative Committee (CCITT).

In addition to the above industry standards, the Network Management Forum has developed a set of pertinent specifications. The following documents are available from:

Network Management Forum (NMF)
1201 Mt. Kemble Avenue
Morristown, NJ 07960-6628

Documents:

(1) *OMNIPoint 1 Specifications*, 1993, and OMNIPoint 1+, 1994.

(2) *Service Provider Integrated Requirements for Information Technology (SPIRIT)*, Issue 2.0, 1994.

(3) Network Management Forum: Forum 026, *Translation of Internet MIBs to ISO/CCITT Guidelines for the Definition of Managed Objects (GDMO) Management Information Bases (MIBs)*, Issue 1.0, Oct 93.

(4) Network Management Forum: Forum 027, *ISO/CCITT to Internet Management Security*, Issue 1.0, Oct 93.

Electronic ftp retrieval
Remote host = thumper.bellcore.com Path/filename = pub/forum/iimc/

(5) Network Management Forum: Forum 028, *ISO/CCITT to Internet Management Proxy*, Issue 1.0, Oct 93.

Electronic ftp retrieval
Remote host = thumper.bellcore.com Path/filename = pub/forum/iimc/

(6) Network Management Forum: Forum 029, *Translation of Internet MIB-II (RFC-1213) to ISO/CCITT GDMO MIB*, Issue 1.0, Oct 93.

Electronic ftp retrieval
Remote host = thumper.bellcore.com Path/filename = pub/forum/iimc/

(7) Network Management Forum: Forum 030, *Translation of ISO/CCITT GDMO MIBs to Internet MIBs*, Issue 1.0, Oct 93.

Electronic ftp retrieval
Remote host = thumper.bellcore.com Path/filename = pub/forum/iimc/

R.2.2 Internet Publications

An Internet Architecture Board (IAB) standard is published as an IAB STD. An IAB standard is published as a Request for Comment (RFC) document. In addition to the RFCs listed below, draft and proposed RFCs are developed and distributed for comments. RFC 1500 is an index to all RFCs. These documents are available from:

DDN Network Information Center
14200 Park Meadow Drive
Suite 200
Chantilly, VA 22021
(800) 365-3642 or (703) 802-4535
unclass e-mail at nic@nic.ddn.mil

Electronic retrieval of RFCs are from the same remote host, ds.internic.net, and the path/filename is rfc####.txt where #### is the 4-digit RFC number.

Documents:

(1) RFC 1500, *Internet Official Protocol Standards*, Aug 93.

(2) RFC 1155, *Structure of Management Information (SMI)*, May 90.

(3) IAB STD 15 (RFC 1157), *Simple Network Management Protocol (SNMP)*, May 90.

(4) RFC 1212, *Concise MIB Definitions*.

(5) IAB STD 17 (RFC 1213), *Management Information Base - II (MIB-II)*, Mar 91.

(6) RFC 1271, *Remote Monitoring Management Information Base (RMON MIB)*, Nov 91.

(7) RFC 1441, *Introduction to version 2 of the Internet-standard Network Management Framework*, Apr 93.

(8) RFC 1442, *Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr 93.

(9) RFC 1443, *Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr 93.

(10) RFC 1444, *Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr 93.

(11) RFC 1445, *Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr 93.

(12) RFC 1446, *Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr 93.

(13) RFC 1447, *Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr 93.

(14) RFC 1448, *Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr 93.

(15) RFC 1449, *Textual Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr 93.

(16) RFC 1450, *Management Information Base of version 2 of the Simple Network Management Protocol (SNMPv2)*, Apr 93.

(17) RFC 1451, *Manager-to-Manager Management Information Base*, Apr 93.

(18) RFC 1452, *Coexistence between version 1 and version 2 of the Internet-standard Network Management Framework*, Apr 93.

Appendix A: SIPRNET Site Listing and Topology Maps

This appendix provides information concerning the DISN SIPRNET WAN. Because the GCCS uses the SIPRNET for it primary WAN datagram transport, it is important that GCCS users understand this DISN network. Included in the appendix will be a table showing the SIPRNET WAN router locations followed by topology maps that were current at the time of this document's publication. Current information on the SIPRNET can be obtained from the SIPRNET Project Officer by contacting the DISA/D343 office at commercial (703)-735-8290 or DSN 653-8290.

Table A1 identifies the SIPRNET WAN locations. The first column identifies the SIPRNET router location. The second column is the Node ID associated with that DISN asset. The third column identifies the core IP address associated with that router. The fourth column is the operational status of the WAN site. The fifth and sixth columns identify what type of Cisco router the node is and in which theater it is located. The final column, Notes, identifies changes planned for any of the locations. Most Notes reflect what type of router the location will receive as the SIPRNET is upgraded over the next year.

Figures A1, A2, and A3 on the following pages show the SIPRNET topology maps. The maps were current on 17 March 1996.

Location	Node ID	IP Address	Current Status	Device	Theatre	Notes
STERLING	SPRW.170	140.049.170.000	OPERATIONAL	AGSPLUS	WESTHEM	7000
NORFOLK-1	SPRW.171	140.049.171.000	OPERATIONAL	7000	WESTHEM	7507
FT MCPHERSON	SPRW.172	140.049.172.000	OPERATIONAL	7000	WESTHEM	7000
SCOTT AFB-1	SPRW.173	140.049.173.000	OPERATIONAL	7000	WESTHEM	7513
MACDILL AFB-1	SPRW.174	140.049.174.000	OPERATIONAL	7000	WESTHEM	7513/7000
FT BELVOIR-1	SPRW.175	140.049.175.000	OPERATIONAL	7000	WESTHEM	7513
FT HUACHUCA	SPRW.176	140.049.176.000	OPERATIONAL	AGSPLUS	WESTHEM	7507
PETERSON AFB	SPRW.177	140.049.177.000	OPERATIONAL	7000	WESTHEM	7507
COROZAL	SPRW.178	140.049.178.000	OPERATIONAL	AGSPLUS	WESTHEM	7507
HICKAM AFB	SPRP.179	140.049.179.000	OPERATIONAL	AGSPLUS	PACIFIC	7507
CROUGHTON AB	SPRE.180	140.049.180.000	OPERATIONAL	AGSPLUS	WESTHEM	7507
RAMSTEIN AB	SPRE.181	140.049.181.000	OPERATIONAL	7000	EUROPE	7507
VAIHINGEN-1	SPRE.182	140.049.182.000	OPERATIONAL	AGSPLUS	EUROPE	7505
ARLINGTON	SPRW.183	140.049.183.000	OPERATIONAL	7000	WESTHEM	
SITE-R	SPRW.184	140.049.184.000	OPERATIONAL	AGSPLUS	WESTHEM	7507
OSAN-AB	SPRP.185	140.049.185.000	OPERATIONAL	AGSPLUS	PACIFIC	7507
FT SHAFTER	SPRP.186	140.049.186.000	OPERATIONAL	AGSPLUS	PACIFIC	7507
FT BUCKNER	SPRP.187	140.049.187.000	OPERATIONAL	AGSPLUS	PACIFIC	7507
PENTAGON-1	SPRW.188	140.049.188.000	OPERATIONAL	7000	WESTHEM	7507
HANCOCK AAF	SPRW.189	140.049.189.000	OPERATIONAL	AGSPLUS	WESTHEM	7507
MCCLELLAN AFB	SPRW.190	140.049.190.000	OPERATIONAL	7000	WESTHEM	DEINSTALL
SAN DIEGO	SPRW.191	140.049.191.000	OPERATIONAL	7000	WESTHEM	
ELMENDORF AFB	SPRP.192	140.049.192.000	OPERATIONAL	AGSPLUS	PACIFIC	7505
WAHIAWA	SPRP.193	140.049.193.000	OPERATIONAL	AGSPLUS	PACIFIC	7507
YOKOTA AB	SPRP.194	140.049.194.000	OPERATIONAL	AGSPLUS	PACIFIC	7507
CAPODICHINO	SPRE.195	140.049.195.000	OPERATIONAL	AGSPLUS	EUROPE	7507
BAHRAIN	SPRE.196	140.049.196.000	OPERATIONAL	AGSPLUS	EUROPE	7507
HEIDELBERG	SPRE.197	140.049.197.000	OPERATIONAL	AGSPLUS	EUROPE	7507
TAEGU AB	SPRP.198	140.049.198.000	OPERATIONAL	AGSPLUS	PACIFIC	7507
MACDILL AFB-2	SPRW.199	140.049.199.000	OPERATIONAL	AGSPLUS	WESTHEM	DEINSTALL/7507
CARLISLE BARRACKS	SPRW.200	140.049.200.000	OPERATIONAL	AGSPLUS	WESTHEM	7507
FT RITCHIE	SPRW.201	140.049.201.000	OPERATIONAL	AGSPLUS	WESTHEM	DEINSTALL
RIYADH	SPRE.202	140.049.202.000	OPERATIONAL	AGSPLUS	EUROPE	7507
NUERNBERG	SPRE.203	140.049.203.000	OPERATIONAL	AGSPLUS	EUROPE	7507
AVIANO AB	SPRE.204	140.049.204.000	OPERATIONAL	AGSPLUS	EUROPE	7507
FT LEWIS	SPRW.205	140.049.205.000	INSTALLED	7000	WESTHEM	
KELLY AFB	SPRW.206	140.049.206.000	OPERATIONAL	7000	WESTHEM	
FINEGAYAN	SPRP.207	140.049.207.000	OPERATIONAL	AGSPLUS	PACIFIC	7505
PENTAGON-2	SPRW.208	140.049.208.000	OPERATIONAL	7000	WESTHEM	7507
FT BRAGG	SPRW.209	140.049.209.000	OPERATIONAL	AGSPLUS	WESTHEM	7507
YONGSAN AB	SPRP.210	140.049.210.000	OPERATIONAL	AGSPLUS	PACIFIC	7507
WHEELER AAF	SPRP.211	140.049.211.000	OPERATIONAL	AGSPLUS	PACIFIC	7505
SCOTT AFB-2	SPRW.212	140.049.212.000	OPERATIONAL	7000	WESTHEM	DEINSTALL
FT BELVOIR-2	SPRW.213	140.049.213.000	PLANNED	7000	WESTHEM	DEINSTALL
DHAHRAN	SPRE.214	140.049.214.000	OPERATIONAL	4500	EUROPE	
LONDON	SPRE.215	140.049.215.000	OPERATIONAL	AGSPLUS	EUROPE	7507
HAMPTON ROADS	SPRW.216	140.049.216.000	PLANNED	7000	WESTHEM	
FT MONMOUTH	SPRW.217	140.049.217.000	INSTALLED	7010	WESTHEM	
NORFOLK-2	SPRW.218	140.049.218.000	CANCELLED	7000	WESTHEM	CANCELLED
MONTEREY	SPRW.219	140.049.219.000	OPERATIONAL	7000	WESTHEM	
ANDREWS AFB	SPRW.220	140.049.220.000	CANCELLED	7000	WESTHEM	CANCELLED
VAIHINGEN-2	SPRE.221	140.049.221.000	PLANNED	7000	EUROPE	
COLUMBUS-1	SPRW.222	140.049.222.000	PLANNED	4500	WESTHEM	
KAPOSVAR	SPRE.223	140.049.223.000	OPERATIONAL	AGSPLUS	EUROPE	
TUZLA-1	SPRE.224	140.049.224.000	OPERATIONAL	AGSPLUS	EUROPE	
LUKAVAC	SPRE.225	140.049.225.000	OPERATIONAL	AGSPLUS	EUROPE	
COLUMBUS-2	SPRW.228	140.049.228.000	PLANNED	4500	WESTHEM	
BEALE AFB	SPRW.229	140.049.229.000	PLANNED	7000	WESTHEM	7507

Table A1 SIPRNET Router Locations

SIPRNET Topology Map - Continental United States

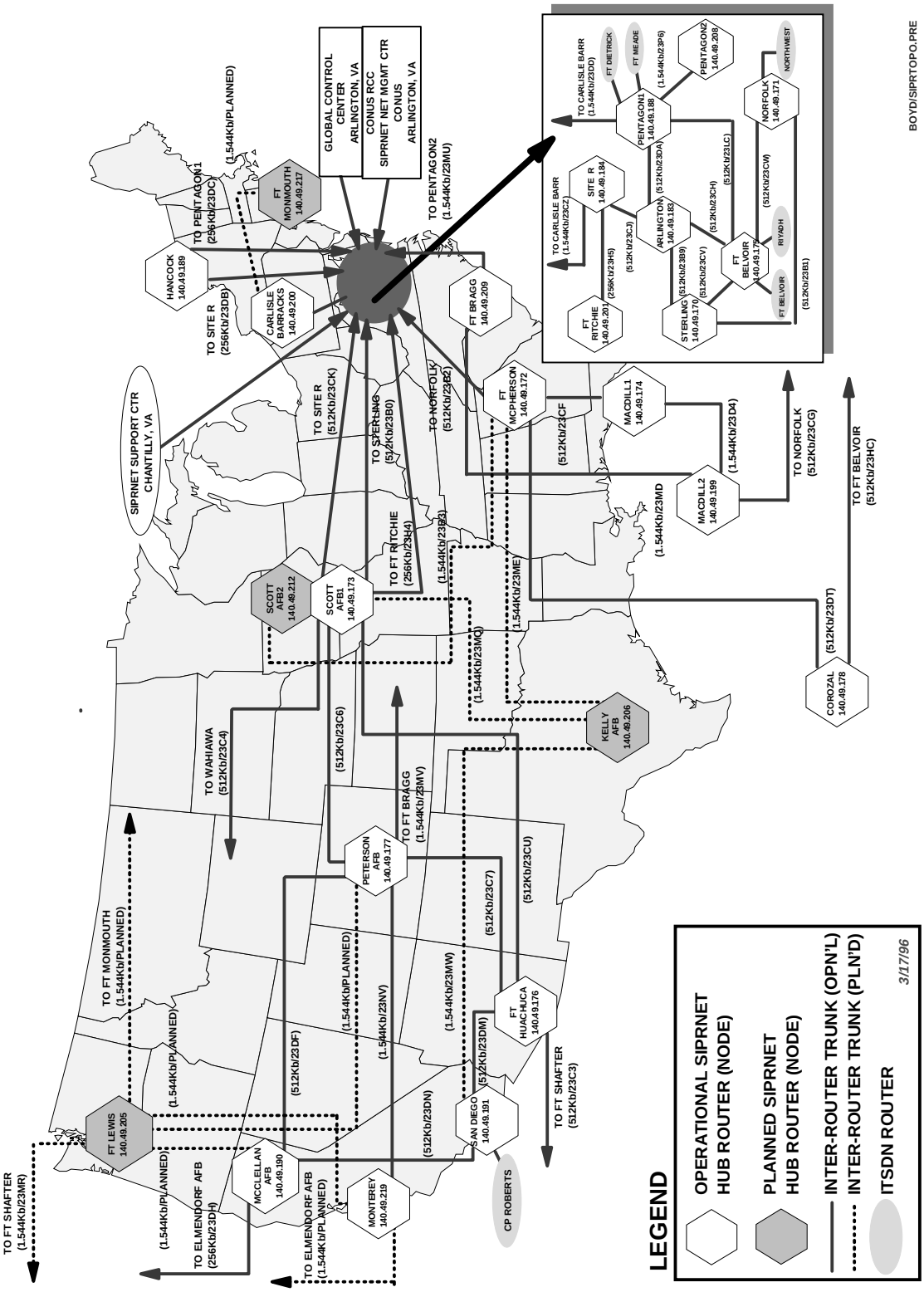


Figure A1 SIPRNET CONUS Topology Map

SIPRNET Topology Map - Pacific Theater

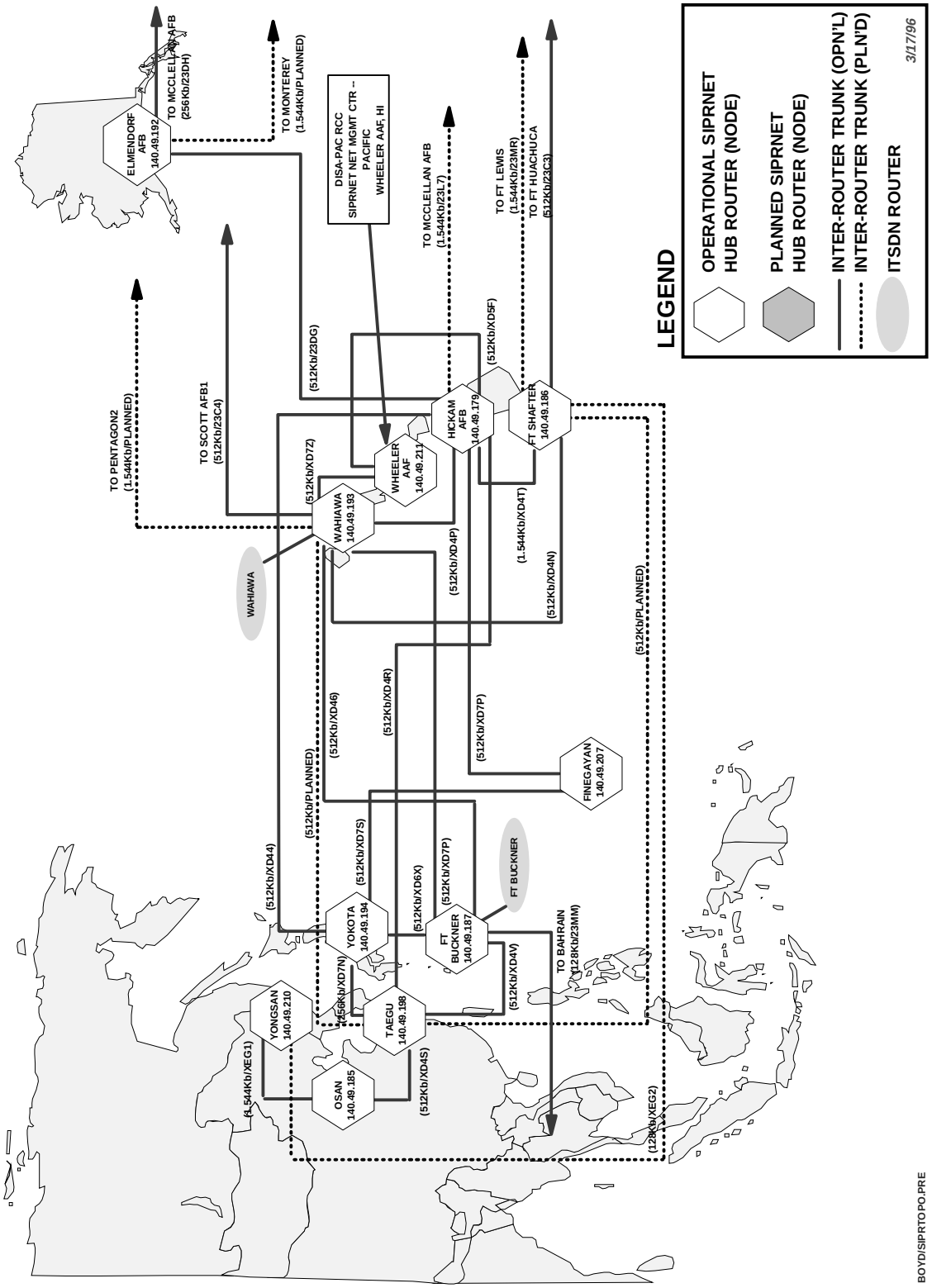


Figure A2 SIPRNET Pacific Theater Topology Map

SIPRNET Topology Map -European Theater

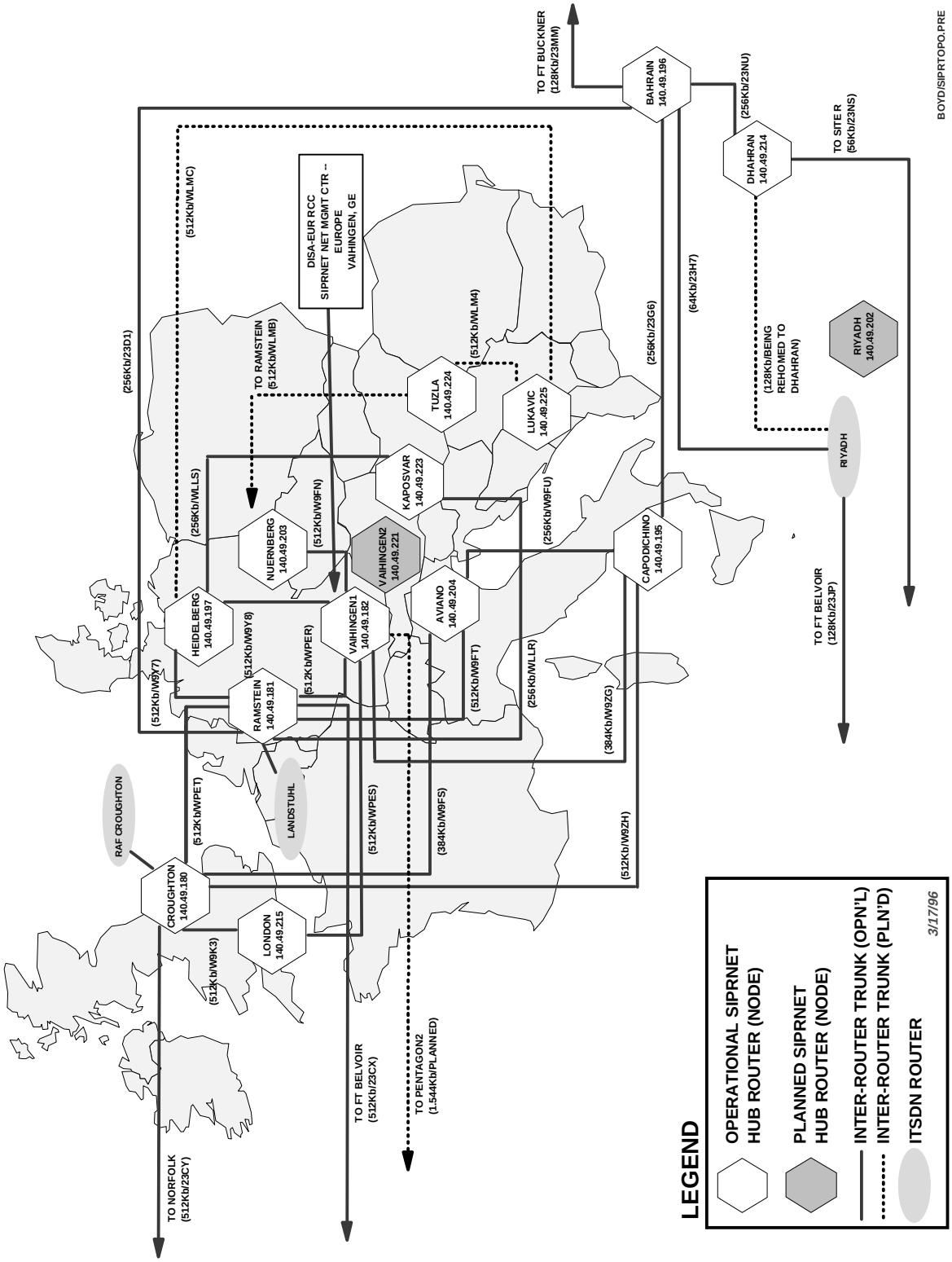


Figure A3 SIPRNET European Theater Topology Map

Appendix B: The Integrated Tactical Strategic Data Network (ITSDN) Program

B.1 General

The ITSDN gateway routers will be used to support deployed Joint Task Force (JTF) contingencies that have requirements to operate with routers. The ITSDN program installed routers at 10 different strategic entry points. The 20 gateway routers are divided into two sets of 10 routers each based on the classification of data they process. The first set of routers will connect the tactical subscriber to strategic networks via the SIPRNET. The other set of routers will connect the tactical subscriber to strategic networks via the NIPRNET. Each entry point has received two routers, one unclassified and the other secret. SIPRNET and NIPRNET are two of the four IP router layers defined in the DISN router architecture model.

The ITSDN entry point suite of equipment consists of an unclassified router, a secret router, cryptographic equipment, and other ancillary devices. The 10 suites of equipment allow tactical forces access to strategic systems via the Defense Satellite Communications System (DSCS) through a Defense Communications System Entry Point (DCS-EP). The ITSDN gateways at the EPs provide world wide NIPRNET and SIPRNET access for the JTFs and are able to support at least two contingency operations in different parts of the world simultaneously. Some documents being produced may refer to the DCS-EPs as Defense Information System Network Entry Points (DISN-EPs). Both are valid. Additionally, the DCS-EPs are undergoing upgrades. Once an upgrade is complete, the location is considered a DISN Standardized Tactical Entry Point (STEP).

B.2 Addressing Considerations

Tactically-fielded service/component force element networks are provided serial connectivity into the ITSDN gateways via satellite communications equipment at the DCS-EP sites. Each of the ITSDN gateways are considered as separate autonomous systems, that is, these gateways are not considered or included as part of the interior networks of any of the strategic or tactical client networks that they serve. It is therefore necessary for all client networks to use an exterior gateway protocol to communicate with the ITSDN gateway. The exterior gateway routing protocol that will be used to communicate through the ITSDN gateway, at least initially, will be Transmission Control Protocol/Internet Protocol's (TCP/IP's) Exterior Gateway Protocol (EGP), in conjunction with the wide area networking protocols, Point-to-Point Protocol (PPP) or X.25. All ITSDN gateway router ports are preconfigured with the PPP and EGP protocols. The X.25 protocol will be configured upon request. The ITSDN addressing calls for the initial use of EGP-3 and the later introduction of Border Gateway Protocol (BGP), Version 4 (BGP-4). However, BGP-4 can be configured upon request. Because of the shortcomings in existing exterior protocols, a two phased approach for addressing the ITSDN gateway routers is used. Phase I will use a unique class C network number per router port. This phase requires 280 class C network numbers. BGP-4 can be configured during Phase I address implementation. Phase II will use a single class C network number per router. This approach requires only 20 class C network numbers. Phase II will be implemented after all routers and tactical networks migrate to and can support BGP-4. BGP-4 is designed to support a subnetted,

multi-vendor environment. Complete information concerning the specifics of network addressing for the ITSDN Program can be obtained from DISA's DISN Networks Branch (D343) and JIEO Center for Systems Engineering's JTF Support Branch (JEECC).

Deployed tactical forces operate in a very dynamic environment. Several problems occur from this environment that must be factored into determining the proper approach to network addressing. Tactical subscribers very likely will move as an engagement changes. Failures at DCS entry points may require tactical users to down-link into a different DCS entry point. Multiple JTFs may be operating at the same time against different adversaries. Two JTFs may require an interface to the same DCS-EP. Some DCS-EPs are dual nodes while others are single node operations. Each of these scenarios must be factored into the final plan.

The gateway routers are configured with 14 interface ports, 13 serial and 1 Ethernet ports. Routers make no distinction between trunk ports and access (subscriber/user) ports except with regard to the physical/electrical characteristics of the interface (ethernet, low-speed serial, or high-speed serial). Similarly, routers make no distinction between trunk IP addresses and access IP addresses. An IP address identifies a specific router port, but the address generally has no relationship to the type of port, trunk, or access circuit (serial or ethernet). While this provides a great deal of flexibility in selecting addressing schemes, it also requires a high degree of configuration management and control to deploy network numbers properly. Incorrect address assignments initially may go undetected, but eventually they will lead to catastrophic network failures.

B.3 ITSDN Gateway Router Locations

Deployed forces normally access the DISN from their tactical location using satellite communications. The five areas of satellite coverage defined by DSCS satellites are the: Indian Ocean (IO); West Pacific (WP); East Pacific (EP); WestLant (WL); and EastLant (EL). Table B1 lists the DCS-EPs and the appropriate geographical area covered by the satellite. Access to NIPRNET or SIPRNET routers at the DCS gateway station EPs is operationally controlled by the appropriate DISA's Theater Contingency Operations Branches (D333, PC321, and EU333). Users requesting ITSDN gateway router access must include the required configuration in the user's request for DCS gateway station access.

Site:	Satellite Nodes:	IO	WP	EP	WL	EL
Wahiawa	2		X	X		
Ft Detrick	2			X	X	
Ft Meade	2			X		X
Croughton	1					X
Landstuhl	2	X			X	
Northwest	2				X	X
Ft Buckner	2	X	X			
Cp Roberts	2		X	X		
Ft Belvoir	2			X	X	
Riyadh	1					X

Table B1 DCS Entry Points and DSCS Satellite Coverage

The ITSDN gateways are dedicated to the CINC and his Component Force Elements during contingencies, exercises, and training missions. They are not for sustained operations. The tactical subscribers access to the ITSDN gateways is funded through the Defense Budget Operating Fund (DBOF) provided the requirement is validated by the appropriate CINC J-6. The DISA Theater Contingency Operations Branches (D333, EU333, PC321) provide direction to the theater RCCs and DCS-EPs on utilization of the ITSDN gateways. The customer (i.e., tactical data user), in concert with the Theater Contingency Operations Branch, will gain ITSDN gateway access only as a part of a JTF after CINC J-6 validation. The RCC's work directly with the customer, Theater Contingency Operations Branches, and DCS Entry Points to control the operational configuration of the ITSDN gateways and achieve interoperability of the customer's tactical network to the NIPRNET and the SIPRNET. The ITSDN nodes are standardized and pre-configured with a multi-protocol capability to support the warfighter.

The DCS-EPs are divided into two categories, dual node sites and single node sites. The dual node sites have redundant satellite stations. The different ITSDN gateway router ports are designated Subscriber #1, Subscriber #2, and so forth. The GCC will assign JTF tactical users to subscriber positions during the JTF buildup phase.

Single node sites will receive gateway routers with the same hardware and software configuration as the dual node sites. While the DCS-EP data transmission layer cannot support the additional router ports, alternate communication paths may be available. The alternate communications path could come in a variety of forms. One form might be tactical satellite equipment that is temporarily installed at the DCS-EP in support of a crisis. Another could be the lease of commercial satellite equipment

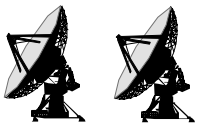
utilized at the DCS-EP. Whatever alternate path might exist, the spare router ports will be addressed and available for use.

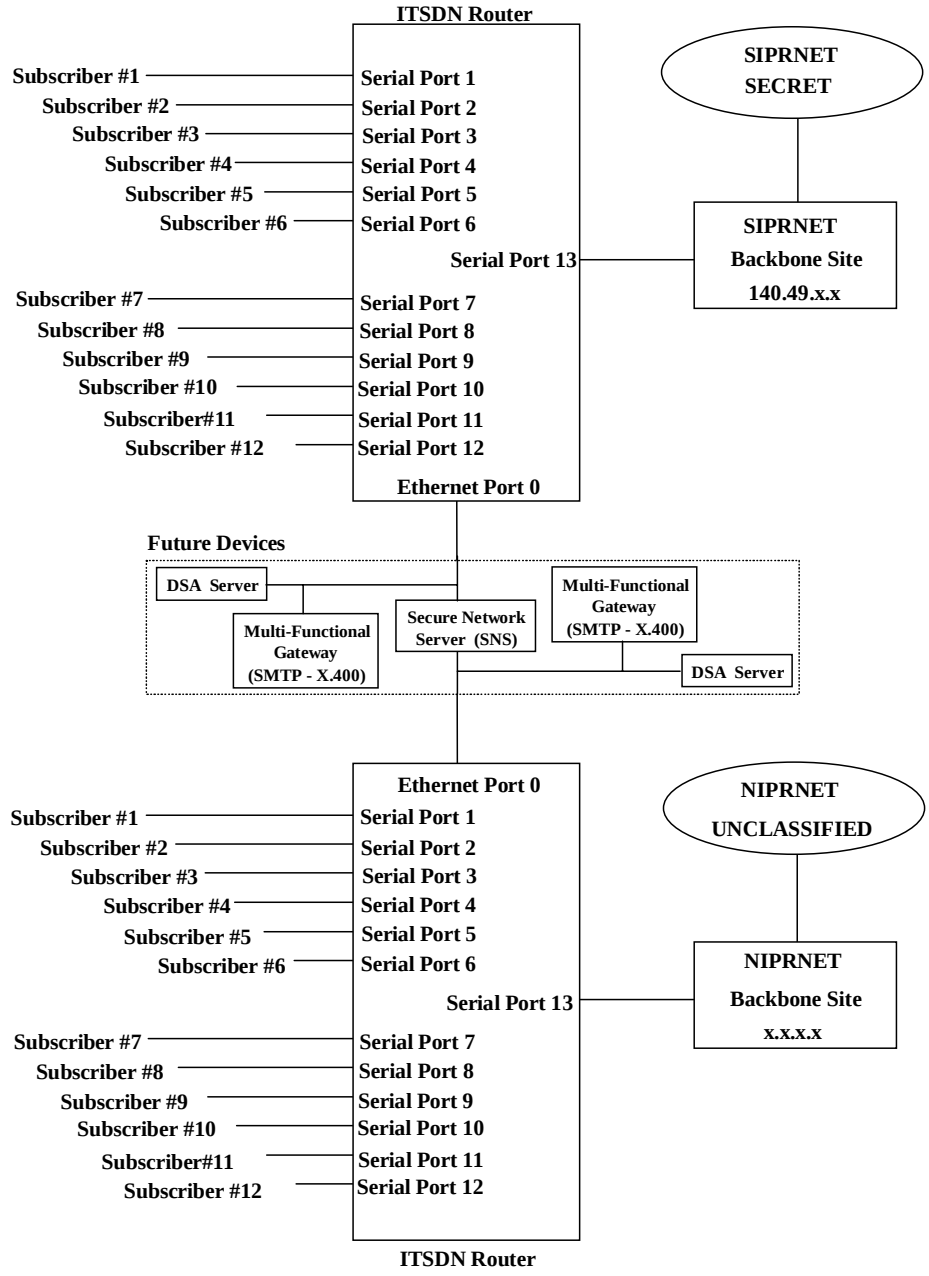
Figures B1 and B2 show how the ITSDN entry point will link the tactical subscribers to the strategic networks. Transmission systems and media have not been shown to simplify the drawings. Figure B1 depicts a dual node site while figure B2 represents a single node site.

ITSDN DCS Entry Point Router Configuration
Dual Satellite Node

Wahiawa, Ft Detrick, Ft Meade, Landstuhl,
Northwest, Ft Buckner, Camp Roberts, Ft Belvoir

Strategic ITSDN Gateway





Joint Task Force subscribers assigned to ports by the Level I Network Ops Center

Figure B1 ITSDN Dual Satellite Node Example

ITSDN DCS Entry Point Router Configuration
Single Satellite Node

Croughton, Riyadh

Strategic ITSDN Gateway

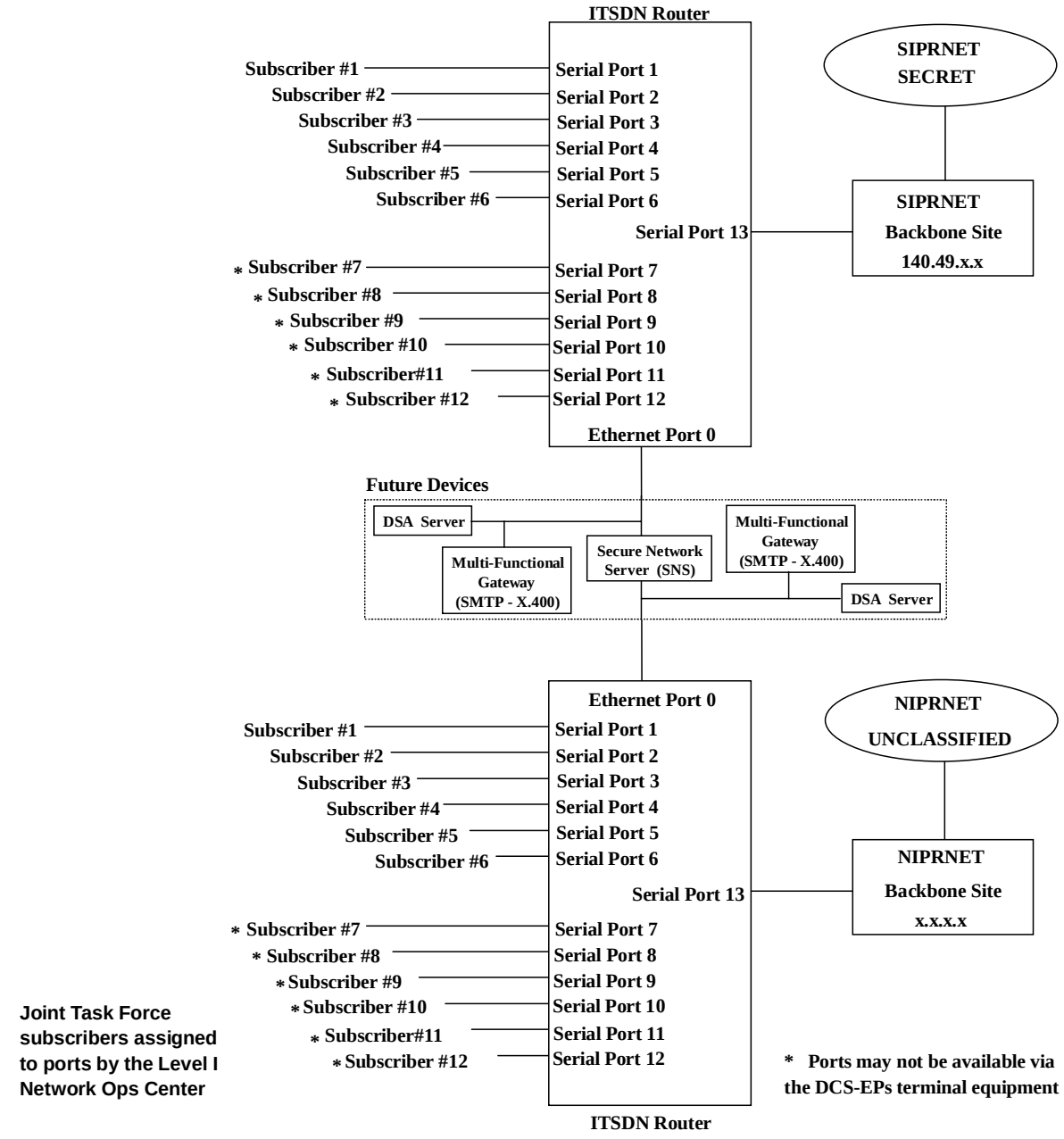


Figure B2 ITSDN Single Satellite Node Example

B.4 ITSDN to SIPRNET Connectivity

Table B2 identifies the secret level ITSDN gateway router locations and their homings to the SIPRNET WAN. The first column identifies the ITSDN router site. The second column is the supporting SIPRNET WAN router location. The next two columns identify the type of connection between the ITSDN router and the SIPRNET WAN router. Each ITSDN gateway is operational.

ITSDN Site:	SIPRNET Site:	Type Connection:	Connection Speed (kbps):
Wahiawa	Wahiawa	Ethernet	10,000
Ft Detrick	Pentagon	Serial	512
Ft Meade	Pentagon	Serial	512
Croughton	Croughton	Ethernet	10,000
Landstuhl	Ramstein	Serial	512
Northwest	Norfolk	Serial	512
Ft Buckner	Ft Buckner	Ethernet	10,000
Cp Roberts	San Diego	Serial	512
Ft Belvoir	Ft Belvoir	Ethernet	10,000
Riyadh	Riyadh	Ethernet	10,000

Table B2 ITSDN Secret Gateway Routers to SIPRNET IP Addresses, Serial Connections

Figure B3 is a graphical depiction of Table B2. The diagram shows how the 10 ITSDN routers are connected to their supporting SIPRNET WAN router. The Landstuhl ITSDN router is expanded in order to show how it could support a deployed JTF. For the example shown each of the six components of the JTF have their own router link back to the strategic world. This will not always be the case. Another example not shown would be that one of the deployed components serves as the focal point for all the other components router needs. In this case only a single router link back to the ITSDN router would be required. A third example would be a mixture of the above two examples. Some components could have their own link back. Other components could piggyback off of a component having a direct link and thus not require their own individual link.

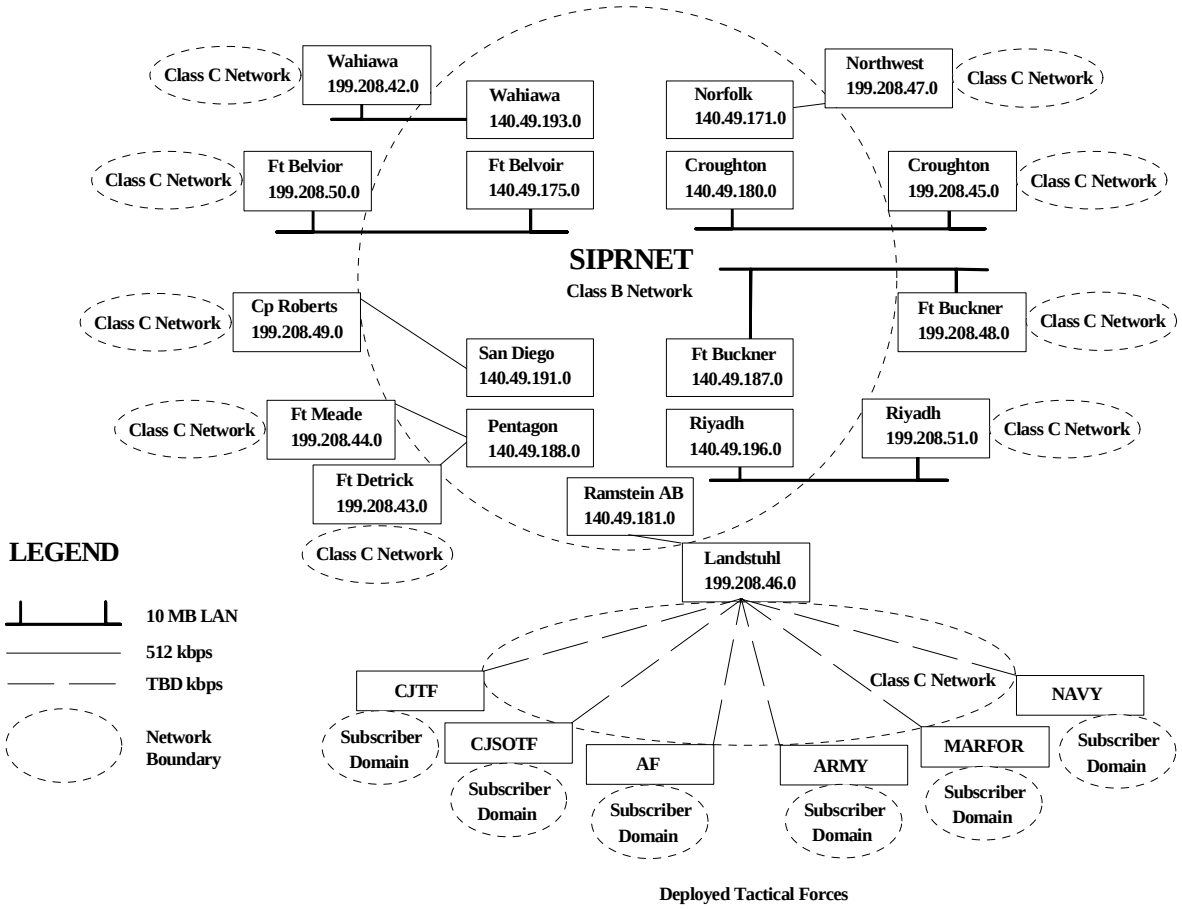


Figure B3 ITSDN Secret Gateway Routers to SIPRNET Diagram, Phase II Addressing Scheme

Additional information on the ITSDN capabilities can be obtained by contacting the DISA/D343 office at commercial (703)-735-8355 or DSN 653-8355.

Appendix C: SIPRNET Communications Servers

Eighteen Cisco 2511 communications servers (2511-CSs) were added to SIPRNET during FY95. The 2511-CSs give the general DoD community the capability to access the SIPRNET network via STU-III dial-in. This will be valuable especially for those remote subscribers who do not have the need for a full time, dedicated connection, for temporarily deployed forces, or for those subscribers who are continually traveling on temporary duty (TDY). In a few, rare instances, a remote subscriber may want a dedicated, full-time, asynchronous connection to the SIPRNET. The 2511-CSs can provide that capability whereas the SIPRNET WAN routers are unable to provide asynchronous connectivity.

The 18 2511-CSs deployed on the SIPRNET are different assets than those being deployed by the GCCS program. The SIPRNET CSs are under the operational control and management of the DII RCCs. They do not belong to the GCCS program.

The remote subscriber tariffs are published in the DISN Rate Structure. Those subscribers registering for dial-in service will pay an initial $45 non-reoccurring fee during registration. The monthly recurring fee is $10 for unlimited usage. The dial-in capabilities used on the DDN (MILNET and DSNET1) are charged on a per packet basis. The DISN rate structure is a major shift in that subscribers are charged based on the bandwidth of the access circuit and not on a per packet basis. Those remote subscribers who use a dedicated, full-time, asynchronous connection to a 2511-CS will be charged differently. Dedicated remote subscribers on a 2511-CS will be charged the DISN router rates, and not the dial-in rate. It will be as if they were connecting to a SIPRNET router. There has been a significant change in tariffs and remote subscribers should closely examine their connectivity requirements.

The SIPRNET CSs will use AT&T STU-III Model 1910 to provide dedicated wireline encryption of the dial-in link. The CSs deployed on SIPRNET are Cisco 2511-CSs which are capable of 112 kbps throughput on the dial in ports. However, the dial in link initially will be limited to a maximum throughput of 19.2 kbps to accommodate all makes and models of compatible secure telephone units in use by the DoD. Higher throughput rates using compression algorithms will be made available on an incremental basis once the initial kbps service has been fielded. A maximum of 38.4 kbps compressed throughput can be realized by newer generation STUs using compression algorithms. The CSs are capable of supporting Telnet, KERMIT, PPP, CPPP, SLIP, CSLIP, and other functions.

Table C1 shows the tentative locations where the 2511-CSs are installed. The first column identifies the 2511-CS site while the second column identifies the country. The third column shows to which SIPRNET WAN router the 2511-CS will be homed. The next two columns identify the type of connection between the 2511-CS and the SIPRNET WAN router and the speed at which this connection will run. Column six identifies if the 2511-CS is up or if it is still in test and acceptance (IT&A). And finally, column seven shows how many STU-IIIs were installed by DISA at the 2511-CS location.

It is important to understand two factors concerning the number of STU-IIIs being deployed by the DISN Data Services Division. The number of STU-IIIs was based on the requirements of the DSNET1 community with some growth expansion factored in. The GCCS program was asked for their dial-in port requirements. The response was that they will deploy their own communication servers. This is why the numbers may appear inadequate without further explanation. Expansion of the number of dial-in ports on the 2511-CSs used on the SIPRNET will be based on the number of registered users. As the number of registered users increases the DISA/D343 office will ensure adequate availability exists. It is a relatively simple process to add more STU-IIIs to those sites with only four installed STU-IIIs.

CS Site	Country	SIPRNET Homing	Type Connection	Connection Speed (kbps)	IOC	Dial in Ports
BAHRAIN	Bahrain	Bahrain -196	Ethernet	10,000	IT&A	4
CAPODICHINO	Italy	Capodichino - 197	Ethernet	10,000	IT&A	4
COROZAL	Panama	Corozal - 178	Ethernet	10,000	IT&A	4
CROUGHTON-RAFB	UK	Croughton - 180	Ethernet	10,000	IT&A	4
ELMENDORF-AFB	US	Elmendorf AFB - 192	Ethernet	10,000	IT&A	4
FINEGAYAN-NAVCAMS	Guam	Finegayan - 207	Ethernet	10,000	IT&A	4
FT-BUCKNER	Japan	Ft Buckner - 187	Ethernet	10,000	IT&A	4
OSF *	US	Sterling - 170	Ethernet	10,000	UP	16
HEIDELBERG	Germany	Heidelberg - 197	Ethernet	10,000	IT&A	4
HICKAM-AFB	US	Hickam AFB - 179	Ethernet	10,000	IT&A	4
MCCLELLAN-AFB *	US	McClellan AFB - 190	Ethernet	10,000	UP	16
MILDENHALL-RAFB	UK	Croughton -180	Serial	64	IT&A	4
RAMSTEIN-AB	Germany	Ramstein AB - 181	Ethernet	10,000	IT&A	4
ROTA-NAS	Spain	Croughton - 180	Serial	64	IT&A	4
TAEGU-CP WALKER	Korea	Taegu - 198	Ethernet	10,000	IT&A	4
VAIHINGEN	Germany	Vaihingen - 182	Ethernet	10,000	IT&A	4
YOKOTA-AB	Japan	Yokota AB - 194	Ethernet	10,000	IT&A	4
YONGSON-AG	Korea	Yongson - 210	Ethernet	10,000	IT&A	4

* These sites will support 1-800 dial in service for SIPRNET in CONUS.

Table C1 SIPRNET Communication Server Locations

The *Defense Information System Network, Dial-In Data Services, Internet Protocol Addressing Plan* was scheduled for publication in July of 1995. This document will describe in detail how the SIPRNET 2511-CSs will be addressed on both the aggregate port and the dial-in subscriber ports. Further information on the dial-in capabilities scheduled for deployment on SIPRNET can be obtained from the DISA/D343 office.

Appendix D: GCCS Communications Servers

Eighty-six Cisco 2511 communications servers (2511-CSs) will be installed at GCCS sites. These 2511-CSs will support the warfighting CINC's remote connectivity requirements for low speed dedicated circuits and STU-III dial-in circuits. The 2511-CSs will provide TCP/IP functionality for remote GCCS users over asynchronous communications lines.

The GCCS 2511-CSs will be under the direction and control of the GCCS sites with overall guidance and management being provided by the GMC. The GCCS Engineering Department will have technical oversight of how the 2511-CSs will be deployed across the GCCS to ensure interoperability across the system and meet mandated security requirements.

Remote GCCS subscribers will not pay a usage fee for using the GCCS communication servers. However, each CINC will be responsible for paying the costs associated with the leased multiplexer circuits supporting the dedicated circuits and the telephone lines used for the dial-in access.

The dial-in lines used by the GCCS must use newer generation STU-IIIs like the AT&T STU-III Model 1910. The STU-IIIs used by the sites must support compressed throughput data rates of 38.4 kbps to adequately run the GCCS applications. Those users connecting via dedicated circuits must use a bandwidth of 32 kbps or greater. Some exceptions do exist for the required bandwidths to operate GCCS applications remotely. Please consult the GCCS Engineering Officer for further information.

The 2511-CSs deployed on the GCCS are capable of 112 kbps throughput on the asynchronous ports. However, the dial in link will be limited to a maximum throughput of 38.4 kbps by the current generation of STU-III devices. The CSs support Telnet, KERMIT, PPP, SLIP, CPPP, CSLIP, and other functions. The GCCS CSs will be configured for SLIP and encapsulated PPP sessions.

The number of CSs required by the GCCS was based on two factors. First several AUTODIN messages were sent from DISA/JIEO to the WWMCCS and GCCS Program Management Offices (PMOs), CINC and S/A GCCS sites, and remote WWMCCS locations. These messages were: Subj: WWMCCS/GCCS Dedicated Remote and Dial-in User Data Call (U), DTG 181134Z APR 95; Subj: Communication Server Rqmts for GCCS (U), DTG 071218A JUN 95; and Remote Connectivity Via GCCS Communication Servers, DTG 162258Z JUN 95. These messages established the number of dedicated circuit and dial-in circuits required by each GCCS CINC or S/A. The second factor was the emergency dial-in management capability required by the GMC to perform effective management of the GCCS. This requirement placed CSs at a few of the GCCS IOC sites that currently do not have dedicated circuit or dial-in users. This gives the GMC an access point should the site become isolated from the network. See Figure D1.

The following table shows the locations where the GCCS 2511-CSs will be installed. The first column identifies the GCCS parent site while the second column identifies the number of 2511-CSs required. The third column shows where the 2511-CS will be installed. Not all 2511-CSs will be

located at the parent site. Many will be installed at other locations and then connected by one of the 2511-CS's serial ports back to the parent site. The next three columns identify the breakdown of the configured asynchronous ports for each 2511-CS. Active ports are divided between those supporting dedicated terminal connections, those operating using STU-III devices, and the dedicated GMC port using a STU-III device. Every port on each 2511-CSs will not be configured. It will depend on the required capabilities at each GCCS location. Determining the data for the missing cells is currently in progress.

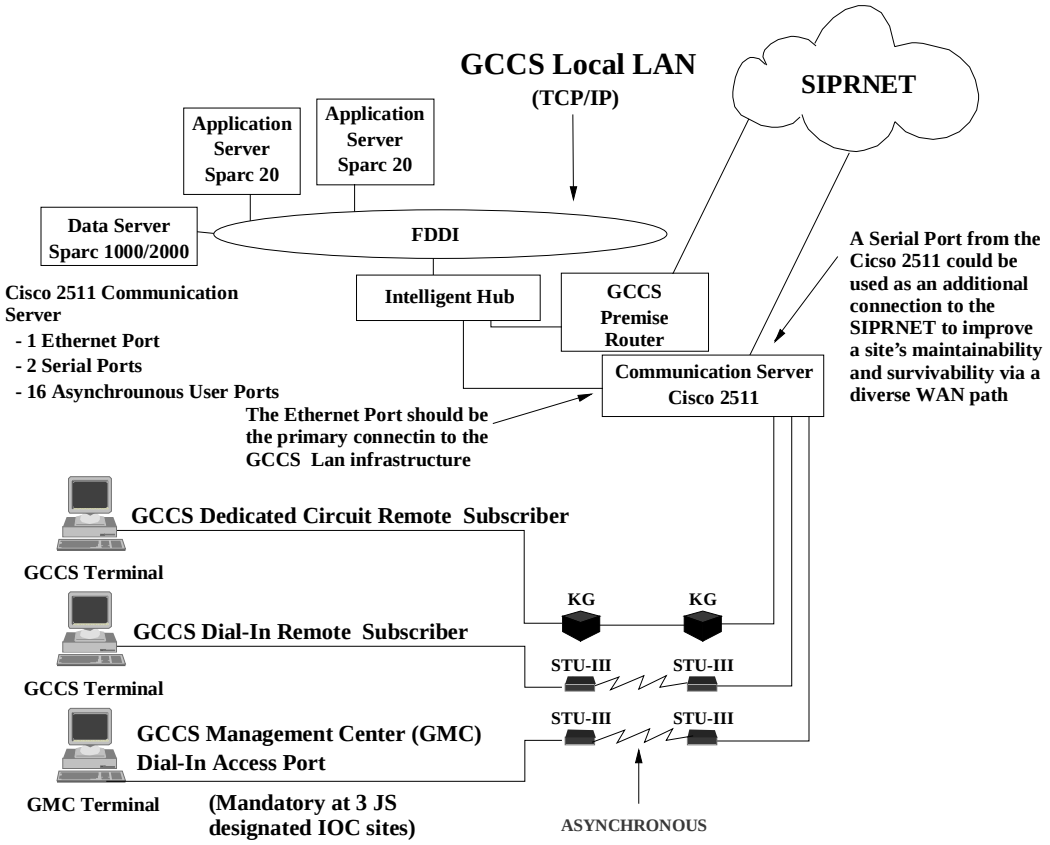


Figure D1 Communication Server User Connections

	GCCS Parent Site	Number of CSs	CS Locations (base/country)	Operational Rqmt	Dedicated Ports	Dial-in Ports	Unused	GMC Ports
1	ACC	5						1
2	AETC (OSF)	1						1
3	AETC (KAFB)	1						1
4	AFMC	1	Wright-Patterson AFB, OH	N	0	0	15	1
5	AFWC	1	Maxwell AFB, AL	N	1	0	0	0
6	AIA	1						1
7	AMC	1	Scott AFB, IL	N	0	16	0	0
8	ANMCC	1	Site R, Ft Ritchie, MD	N	0	0	15	1
9	ARCENT	1	Ft McPherson, GA	N	0	0	15	1
10	AREUR	6	Campbell Bkrs, Heidelberg, Germany	Y	8	4	3	1
			Panzer Kasern, Kaiserslautern, Germany	Y	7	2	7	0
			Kleber Brks, Kaiserslautern, Germany	Y	4	4	8	0
			Camp Ederle, Vicenza, Italy	Y	6	2	8	0
			Unknown (Not shipped)					
			Unknown (Not shipped)					
11	ARPAC	4	Ft Shafter, HI	Y	6	10	0	0
			Ft Shafter, HI	Y	13	3	0	0
			Ft Shafter, HI	Y	16	0	0	0
			Ft Shafter, HI	Y	0	14	1	1
12	ARSPACECOM	2						1
13	AWC (PA)	1						1
14	CENTAF	1	Shaw AFB, SC	N	0	0	15	1
15	CENTCOM	3	MacDill AFB, FL	N	8	8	0	1
			MacDill AFB, FL	N	8	8	0	0
			MacDill AFB, FL	N	8	8	0	0
16	CNO	1	Pentagon, VA	N	6	6	3	1
17	EUCOM	2	Patch Brks, Germany	Y	4	5	6	1
			Patch Brks, Germany	N	4	5	6	1
18	FORSCOM	10	FORSCOM	Y	12			1
			Ft Hood, TX	Y	4			
			Ft Lewis, WA	Y	2			
			Ft Sam Houston, TX	Y	4			
			USARC, GA	Y	4			
			Ft Gillem, GA	Y	10			
			Ft Bragg, NC	Y	2			
			ARCENT, GA	Y	12			
19	HQAF	1	Pentagon, VA	N	0	15	0	1
20	HQDA	4	Pentagon, VA	Y	1	13	1	1
			Pentagon, VA	Y	1	13	2	0
			Pentagon, VA	Y	1	12	3	0
			Pentagon, VA	Y	4	5	7	0

	GCCS Parent Site	Number of CSs	CS Locations (base/country)	Operational Rqmt	Dedicated Ports	Dial-in Ports	Unused	GMC Ports

21	HQMC	1	Navy Annex, VA	N	0	4	11	1
22	JDEF	1						1
23	JTO	1	Joint Training Organization, Scott AFB, IL	N	0	15	0	1
24	MARCENT	1	Camp Pendleton, CA	N	0	3	12	1
25	MARFORLANT	1	Camp Lejeune, NC	N	0	4	11	1
26	MARFORPAC	1	Camp Smith, HI	N	4	0	11	1
27	MSC	1	Washington, DC	N	0	0	15	1
28	MTMC	3	Falls Church, VA	Y	0	4	11	1
			Bayonne, NJ	Y	0	2	14	0
			Oakland Army Base, CA	Y	0	3	13	0
29	NAVCENT FWD	1						1
30	NAVEUR	2	London, England	N	6	6	3	1
			Naples, Italy	Y	12	4	0	0
31	NCTAMS	5	CINCPACFLT, Pearl Harbor, HI	Y	12	0	3	1
			CINCPACFLT, Pearl Harbor, HI	Y	7	7	2	0
			USPACOM, Pearl Harbor, HI	N	6	6	3	1
			USFJ, Yokota AB, Japan	N	6	6	3	1
			USFJ, Yokota AB, Japan	N	6	6	4	0
32	NMCC	1						1
33	OKINAWA	1	III MEF, Camp Butler, Okinawa	N	0	4	11	1
34	PACAF	2	Hickam AFB, HI	N	0	2	13	1
			Unknown (Not Shipped)					
35	QUANTICO	2	Quantico, VA	N	0	4	11	1
			Quantico, VA	N	0	4	12	0
36	SOCOM	2						1
37	SOUTHCOM (W/SPECOPS & USARSO)	4	TBD	TBD	0	1	15	1
			TBD	TBD	TBD	TBD	TBD	0
			Unknown (Not Shipped)					
			Unknown (Not Shipped)					
38	STRATCOM	1	Offutt AFB, NE	N	0	1	14	1
39	TRANSCOM	1	USTRANSCOM, Scott AFB, IL	N	0	15	0	1
40	USACOM	3	USACOM, Norfolk, VA	Y	8	6	1	1
			CINCLANTFLT, Norfolk, VA	Y	12	4	0	0
			CINCLANTFLT, Norfolk, VA	Y	13	3	0	0
41	USAFE	1						1
42	USAMC	1						1
43	USFK	3						1
44	USFK2	3	Taegu, Korea	N	0	5	10	1
			Unknown (Not Shipped)					
			Unknown (Not Shipped)					
45	USSPACECOM	2						1
								0

Table D1 GCCS Communication Server Locations

Appendix E: US Special Operations Command SCAMPI Network

This appendix provides information concerning the US SOCOM SCAMPI network. Information has been taken from the *SCAMPI Services Summary, Headquarters, United States Special Operations Command, December 1994*, document. Considering the age of the document and how fast communications infrastructures are changing, it is recommended current information be obtained from USSOCOM.

E.1 Introduction

SCAMPI is a telecommunications system created to allow dissemination of command, control, communications and intelligence (C3I) information between the United States Special Operations Command (USSOCOM), its components and their major subordinate units, and selected Government agencies and activities directly associated with the special operations community. SCAMPI is not an acronym; it is the term identified with this telecommunications capability. SCAMPI is a closed community system of communications nodes and is the principal C3I medium for USSOCOM. SCAMPI provides gateway service for the special operations community to external DoD classified voice, data and video teleconferencing (VTC) systems. Transmission of data between SCAMPI nodes is over Defense Information Technology Contracts Office (DITCO) leased T1 and fractional T1 (FT1) lines. SCAMPI carries collateral (red) and sensitive compartmented information (SCI) (grey) voice and data. Voice and data information are integrated into data streams using multiplexers (MUXs). All information sent over DITCO leased lines is fully secured using one or two levels of encryption. This summary describes SCAMPI, the network configuration and current services.

E.2 Security Guidance

Information transmitted over SCAMPI is fully secured through the classification level of top secret (TS). Classification categories of collateral (sometimes used synonymously with General Service (GENSER)) and SCI are available on SCAMPI. SCI information and collateral information are separately encrypted and transmitted over a single integrated transmission path.

SCAMPI site locations are, for the most part, unclassified; however, linkage of SCAMPI capability with certain special operations forces is classified SECRET. Most references to SCAMPI locations are to the site rather than the involved activity. Full details regarding classification can be found in the SCAMPI security classification guide that is available from USSOCOM, J6-T.

E.3 SCAMPI Attributes

SCAMPI has the ability to transmit C3I information at multiple security classification levels and provide multimedia services including voice, data, OPSCOM/facsimile, and VTC over a single integrated transmission path. This eliminates the need for multiple single level and dedicated single service systems such as the Defense Secure Network (DSNET 1 and DSNET2), the Defense Red Switched Network (DRSN), the Secret Internet Protocol Router Network (SIPRNET), the Air Force

Network (AFNET) and the DSNET3 which is being replaced by the Joint Worldwide Intelligence Communications System (JWICS).

A single point of contact has been established for all SCAMPI network problems and inquiries. SCAMPI is centrally managed which allows for improved network management and configuration control. SCAMPI consists of a combination of commercial and government off-the-shelf (COTS/GOTS) equipment. SCAMPI is a competitively contracted network. The fiber backbone is provided by one vendor, operations and maintenance by a second, and system engineering and implementation by a third.

SCAMPI is migrating to an architecture based on Integrated Digital Network eXchange (IDNX) MUXs manufactured by Network Equipment Technologies (NET), Inc. The IDNX MUXs support bandwidth-on-demand by allocating bandwidth to services on an as needed basis. Bandwidth is no longer dedicated to and wasted by services in an idle state. The IDNX multiplexer is becoming the Department of Defense (DoD) standard and is being used in other networks, such as the AFNET and the DSNET3/JWICS, making interoperability with these networks easier.

E.4 SCAMPI Network

Information transmitted over SCAMPI is carried in digital form on fiber optic circuits leased by the DITCO. SCAMPI signals conform to the T-carrier format used by the public switched data networks. SCAMPI consists of the circuits, the suites of off-the-shelf equipment that terminate the T-carrier data streams, and the equipment that then splits and reformats the information so that it can be used by user terminal equipment (e.g., telephones, facsimile equipment and micro-computers).

The SCAMPI system currently interconnects 38 sites, also called nodes. Four of these sites are designated as hubs; two located at Ft. Bragg, NC, one at the Pentagon and one at MacDill Air Force Base (AFB), FL. The SCAMPI node designated Fort Bragg Main serves as the controlling hub (CHUB) that provides system management and controls the flow of information within the network. Most nodes connect directly to the hubs. Some nodes connect to the hubs through an intermediate node. The two nodes' signals are combined on the same circuit to minimize circuit costs. When these services are combined, the first node separates its data stream from that of the second node and routes the remaining information on to the second node. These indirectly connected nodes are known as drop and insert nodes. The SCAMPI system architecture is shown in Figure E1, and the SCAMPI system interconnection with service descriptions is shown in Figure E2.

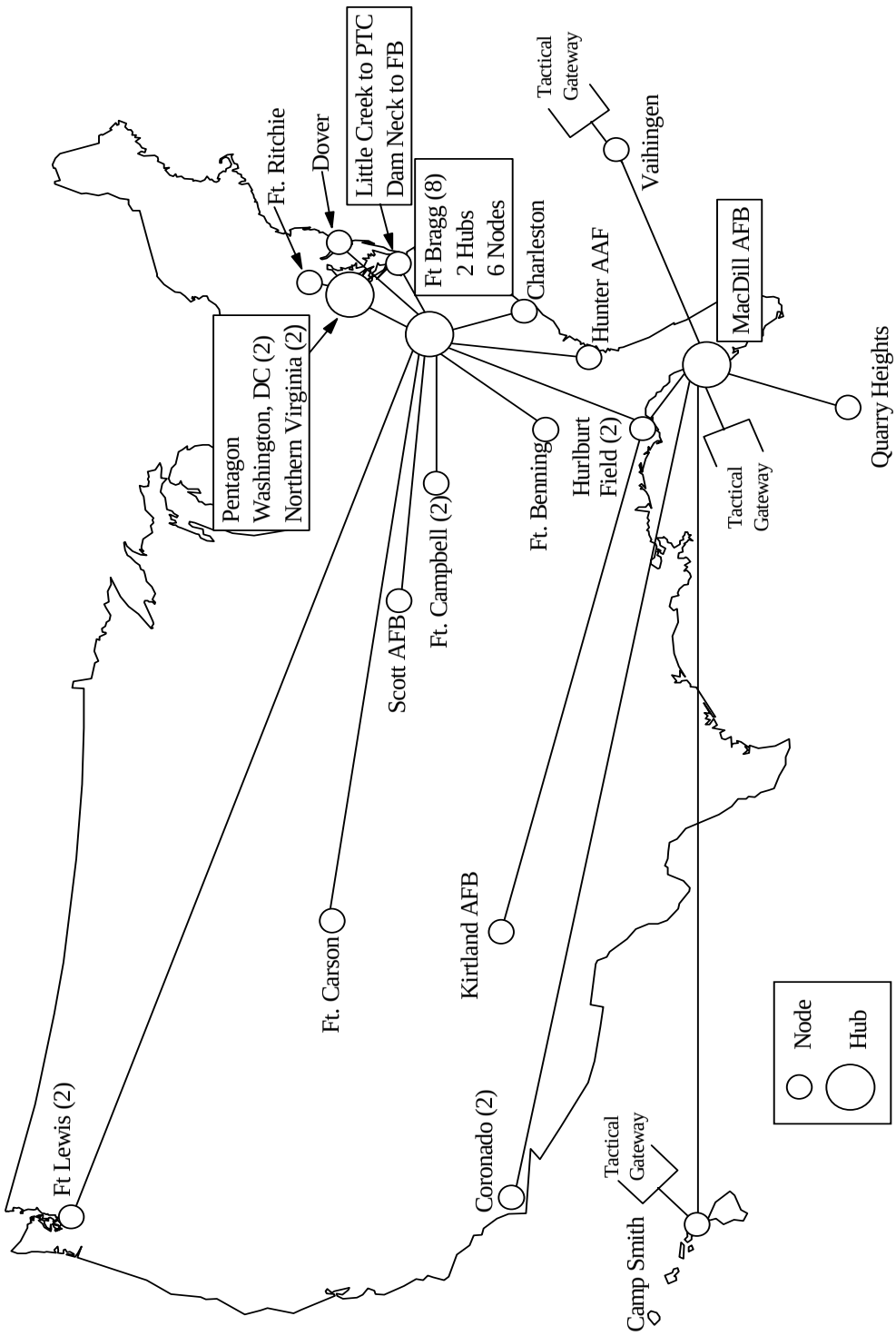


Figure E1 SCAMPI Architecture

Figure E2 SCAMPI System with Node Description and Circuit Interconnection

E.5 Hub/Site Equipment Configurations

Each SCAMPI equipment suite provides service tailored for the user. Users who require collateral and SCI information are provided a full service node. Users who need only collateral or SCI service receive a smaller suite of equipment.

The CHUB site is the center of control for the existing SCAMPI system. It controls all other hubs and nodes. Monitoring and reporting of all system activity is done by the CHUB. It provides the means for centralized reconfiguration of the system to meet changing operational needs, for centralized monitoring of alarm conditions and for coordination with the remote sites and the T-carrier circuit vendor to correct network problems. A hub distributes information to the remote sites. Both voice and data originate at the hub and the remote sites, but all data is transmitted to hub locations and then routed to the remote sites. Hub sites provide the switching functions to interconnect one remote site to another remote site or to allow the broadcast of one data transmission to several remote locations.

There are five types of SCAMPI site equipment configurations: ABT, AT, BT, C and D sites. Sites with ABT configurations, consisting of three racks of equipment, provide SCI (A rack) and collateral (B rack) voice and data services at T1 rates. The third rack (T rack) consists of equipment used for testing purposes. Sites with AT configurations, consisting of two racks of equipment, provide SCI voice and data service at a T1 rate. BT sites, consisting of two racks of equipment, provide collateral voice and data service normally at a FT1 rate. The C rack provides a site with limited SCI services (CA rack) or limited collateral services (CB rack) normally using a 56 Kbps circuit. The CA and CB racks consist of test equipment and the equipment required to provide the limited SCI or collateral services. A dual C rack configuration (CAB rack) provides limited SCI and collateral services using two 56 Kbps circuits. Local extension of SCAMPI system services to other buildings at a site is made using equipment designated as a D rack.

E.6 SCAMPI Services

SCAMPI provides multimedia services including voice, data, facsimile, and VTC in both the collateral and SCI categories at a top secret level. SCAMPI transmits C3I information at multiple security classification levels over a single integrated transmission path. In essence, SCAMPI is two networks, SCI and collateral, riding a single pipe. Separation of the categories is accomplished through the use of cascaded MUXs. The ability to provide multiple services at different classification levels over a single transmission path eliminates the need for dedicated single service networks and multiple single-level systems. A listing of some of the services provide by SCAMPI is shown in Table E1.

Information Type Classification Type ➔	Collateral (red)	Sensitive Compartmented Information (SCI/grey)
Voice	6 Lines	2 Lines
Data		
Broadcast	OPSCOM / Facsimile VTC	OPSCOM / Facsimile VTC
Point-to-Point	**Wide Area Network** Command LAN, GCCS, SIPRNET and DSNET1[1] VTC	**Wide Area Network** SOCRATES, SOIS, JWICS, and DSNET3[2] VTC
Multipoint	VTC	VTC

Definitions:
OPSCOM - Operations Communications
GCCS - Global Command and Control System
SIPRNET - Secret Internet Protocol Router Network
DSNET1 - Defense Secure Network 1
SOCRATES - Special Operations Command Research, Analysis and Threat Evaluation System
SOIS - Special Operations Intelligence System
JWICS - Joint Worldwide Intelligence Communications System
DSNET3 - Defense Secure Network 3

Notes::

(1) All SCAMPI services are cleared to top secret Level, Collateral WAN is limited to secret level to facilitate greater use

(2) Service at a node is normally either SOCRATES or SOIS

.

Table E1 SCAMPI Services

For further information on the SCAMPI please contact USSOCOM. The mailing address is:

CDR, US Special Operations Command
USSOCOM/J6T (SCAMPI Ops)
7701 Tampa Point Blvd
MacDill AFB, FL 33561-5323

Appendix F: Air Force Command and Control Network (AFC2N) WAN

This appendix provides information concerning the AFC2N. Various statements have been included from AFC2N formal program documentation, briefings, and data from the AFC2N web site (now deactivated). Further information on the AFC2N WAN can be obtained from the AFC2N System Program Manager, Major Jerry J. Kanski, DSN 596-5205, at Maxwell AFB-Gunter Annex, Montgomery, Alabama.

F.1 Mission Need Statement

The following excerpt is the Mission Need Statement (MNS) for the AFC2N.

> The overall goal of Air Force Command and Control Networking (AFC2N) is to establish the common AF network infrastructure necessary for passing AF C2 data between commands, their components, and the Global Command and Control System (GCCS) MAJCOM workstations and the MAJCOM C2 host processor, between remote sites and their C2 host at the MAJCOMS, and between AFC2N and the GCCS nodes at unified and major commands. The AFC2N program will also perform centralized budgeting, procurement, management and installation of the communications and operating system hardware and firmware required to establish and support a modern and flexible information exchange backbone. It will be compatible of quickly and inexpensively adapting to changing requirements while supporting the needs of operational AF users in both the joint and AF unique realms. Hardware acquisition will exclusively use COTS, taking advantage of current government contracts as much as possible. Should procurement of hardware not be feasible through an existing government contract, new program specific contracts will be executed to procure COTS hardware compatible with GCCS hardware and technical initiatives. Ensure command and control C2 protection capabilities are inherent in the system design.

F.2 Program Management Directive Excerpts

The Program Management Directive (PMD) for the Air Force Command And Control Networking (AFC2N) Installation is PMD 4117(7) PE 030152, dated 20 Jul 94. The following sections are included to provide more information on the AFC2N WAN. Additional information on the PMD can be obtained from Mr Bob Stanton, SAF/AQK, at DSN 327-3141, or at stanton@aqpo.hq.af.mil.

AFC2N was initiated on 20 Dec 90 as a configuration change to the WWMCCS system, which was in its sustainment phase. As a configuration change to the WWMCCS system it was managed through the System Development Notification (SDN) process. RDT&E and OT&E for AFC2N were conducted by DISA (as JDSSC/JP) in accordance with the SDN process, which requires them to determine the operational impact of all proposed changes to the WWMCCS baseline. The results of this testing led to their recommendation for approval of the LAN SDN (AF-58). The LAN SDN was

validated and approved for installation on 24 May 91 (JCS SDN #191011). The WAN SDN was validated and approved for installation on 18 May 94 (JCS SDN #F93044).

The following objectives are from the AFC2N PMD. They are:

1. Modernization of the existing communications infrastructure used by the Air Force to exercise command and control of its forces is required to meet the current and future needs of operational commanders world wide. WWMCCS, the basic tool used in deliberate planning, crisis response, and deployment of forces engaged in conventional operations, has several deficiencies which are being addressed by its replacement, the Global Command and Control System (GCCS) as well as the AFC2N System Program Office (SPO). The overall goal of AFC2N is to established the common AF network infrastructure necessary for passing AFC2 data between commands, their components, and the Global Command and Control System (GCCS). Specifically to provide AFC2 sites with reliable, secure, high speed communications between MAJCOM workstations and the MAJCOM C2 host processor, between remote sites and their C2 host at the MAJCOMS, and between AFC2N and the GCCS nodes at unified and major commands.

2. The modernized infrastructure provided by the AFC2N SPO will consist of open systems architecture LANs, gateways/routers, WANs, communications processors and interfaces, operating systems and utility software, LAN servers, etc. It will be standardized across the Air Force and will be compatible with the GCCS and WWMCCS hardware and software. No software development is to be required for connection between GCCS and the AFC2N infrastructure, which will be LAN based at each site. COTS MILSTD TCP/IP protocols will be used for interface at the site level for all attached devices (e.g. workstations, servers, database machines, routers). This will ensure compatibility with GCCS. GCCS servers will attach to the Air Force provided secret LANs installed by AFC2N (after WWMCCS downgrade allows downgrade of AFC2N LANs). Current WWMCCS hosts will be attached to the AFC2N LAN for the interim phase out period of WWMCCS using hardware and software provided by DISA at all CINC and component sites scheduled for GCCS. The wide area networking between sites will be supplied by AFC2N and given to DISA for the DISN program. The primary interface into the joint world will be via WWMCCS but will be via GCCS when it is ready to assume that role.

3. The modernization approach taken will allow Air Force sites to execute whatever Joint, Air Force and/or command unique C2 software they require to perform their mission, satisfy evolving and expanding operational requirements, and take full advantage of current communications technology that supports new data processing capabilities. An essential part of modernizing the AF infrastructure is to facilitate future integration of needed capability and provide a modern, flexible information system. This can only be achieved with an infrastructure based on recognized standards and commercial off-the-shelf (COTS) equipment. This will allow adaptation to changing requirements while continuing to provide users support and guaranteeing compatibility with any future joint system.

4. The AFC2N program will also perform centralized budgeting, procurement, management and installation of the communications and operating system hardware and firmware required to establish and support a modern and flexible information exchange backbone. It will be capable of quickly and inexpensively adapting to changing requirements while supporting the needs of operational AF users in both the joint and AF unique realms. Hardware acquisition will exclusively use COTS, taking advantage of current government contracts as much as possible. Should procurement of hardware not be feasible through an existing government contract, new program specific contracts will be executed to procure COTS hardware compatible with GCCS equipment. Hardware selected for the AFC2N will be proven, commercially available hardware compatible with GCCS hardware and technical initiatives.

5. Ensure command and control C2 protection capabilities are inherent in the system design.

F.3 Technical Aspects

Currently, the AFC2N WAN uses the Open Shortest Path First (OSPF) routing protocol and is divided into a backbone (OSPF Area 0) and nine adjacent OSPF areas. The nine additional areas are:

Area 1 (HQ USSPACECOM) Cheyenne Mt AFS
Area 2 (HQ USSTRATCOM) Offutt AFB
Area 3 (HQ AMC) Scott AFB
Area 4 (HQ AFMC) Wright-Patterson AFB
Area 5 (HQ ACC) Langley AFB
Area 6 (HQ USAF) Pentagon
Area 7 (HQ USCENTCOM) MacDill AFB
Area 8 (HQ PACAF) Hickam AFB
Area 9 (HQ AETC) Randolph AFB

The AFC2N used predominantly 256 kbps trunks with some 512 kbps trunks in CONUS and 56 kbps trunks overseas. A few trunks as low as 9.6 kbps in speed are used for remote areas. Most access circuits to the WAN are 56/64 kbps. Eighty AF bases are now connected to AFC2N with 30 more bases expected to be connected by the end of CY96.

A Network Operations Control Center (NOCC) is located at Gunter Annex for AFC2N. The NOCC operates 0600 to 2200 CST, Monday through Friday. The NOCC monitors and manages all routers and circuits of the AFC2N. The NOCC also has the ability to model, simulate, and troubleshoot the WAN network. The NOCC can be reached at DSN 596-5752 or Commercial at (334) 416-5752. No secret-level DoD e-mail address is available.

Current technical information on the AFC2N can be obtained by contacting Capt Daniel C. Stokley, HQ SSG/SIIA, at DSN 596-5205, Commercial at (334) 416-5205, unclassified FAX DSN 596-3325, or unclass e-mail at STOKLEYD@b856S3.SSC.AF.MIL.

F.4 Future Changes

Programmatically and technically, the AFC2N WAN is undergoing major changes. The AF plans to systematically eliminate all of the AFC2N to AFC2N WAN router trunks. The AFC2N will no longer manage and operate a WAN. Instead the AFC2N will use the DISN SIPRNET for all of its long haul, interconnecting service. The AFC2N routers will become the AF C2 interface between the SIPRNET and the base level C2 networks. More current information can be obtained from Major Kanski listed at the beginning of this appendix.

End of Document